Appendix 4.3-1 Contractor’s Solution

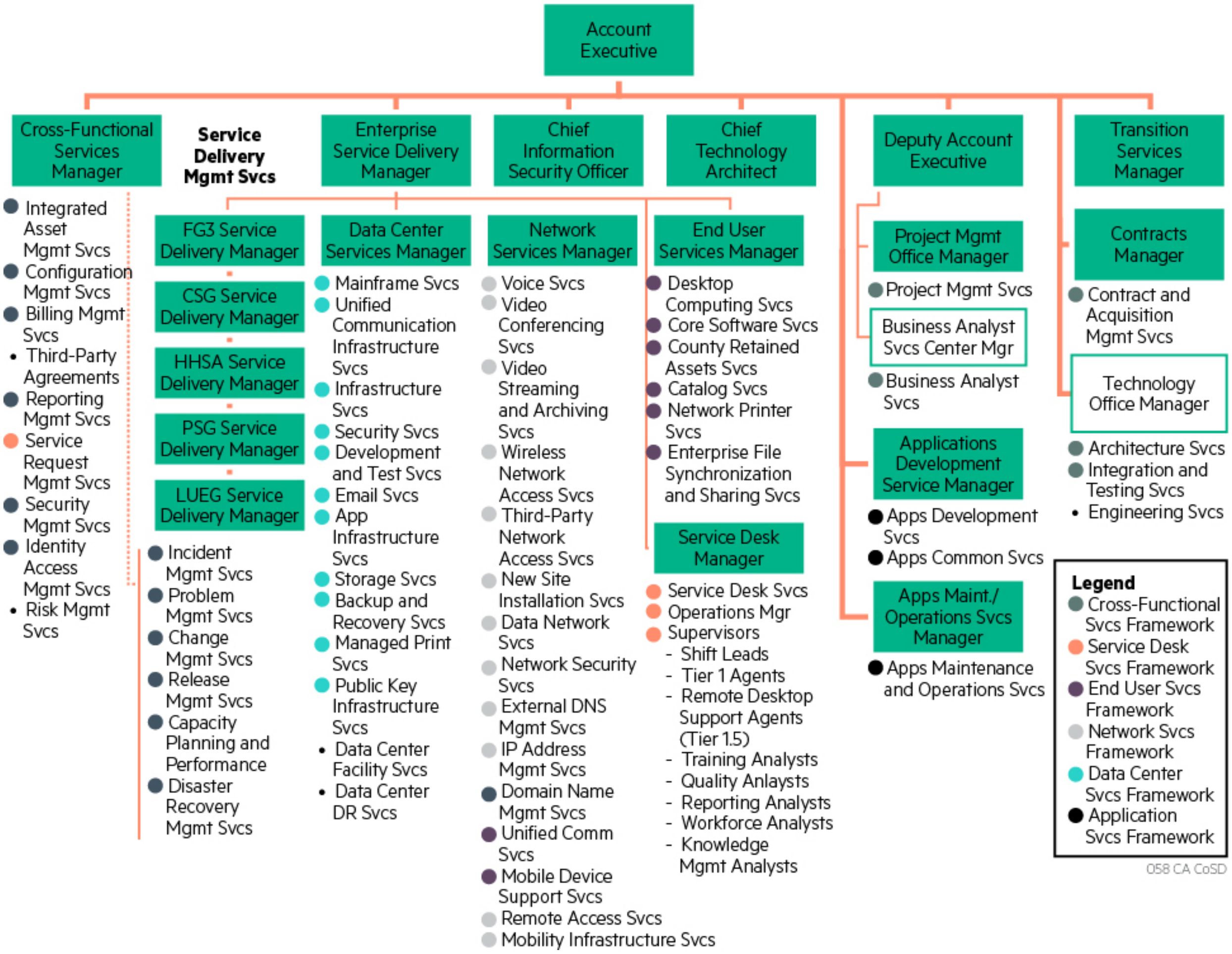
Table of Contents

The following sets forth the Contractor's solution for its performance of the Services under this Agreement. Contractor represents that the solutions set forth below are intended to meet many of the requirements of the Agreement. Nothing in this *Contractor Solutions* shall relieve Contractor of its obligation to perform all Services under the Agreement and to perform the Services in accordance with the standards and requirements set forth in the Agreement.

1. OVERVIEW OF SERVICES

1.1.1. Organization and Staffing

The following organization chart shows Contractor's staffing at a role level and the reporting relationships, including Subcontractors, starting from Account Executive and broken down into Service Frameworks.



Account Executive
Cross-Functional Services Manager
● Integrated Asset Mgmt Svcs
● Configuration Mgmt Svcs
● Billing Mgmt Svcs
• Third-Party Agreements
● Reporting Mgmt Svcs
● Service Request Mgmt Svcs
● Security Mgmt Svcs
● Identity Access Mgmt Svcs
• Risk Mgmt Svcs
Service Delivery Mgmt Svcs
FG3 Service Delivery Manager
CSG Service Delivery Manager
HHSA Service Delivery Manager
PSG Service Delivery Manager
LUEG Service Delivery Manager
● Incident Mgmt Svcs
● Problem Mgmt Svcs
● Change Mgmt Svcs
● Release Mgmt Svcs
● Capacity Planning and Performance
● Disaster Recovery Mgmt Svcs
Enterprise Service Delivery Manager
Data Center Services Manager
● Mainframe Svcs
● Unified Communication Infrastructure Svcs
● Infrastructure Svcs
● Security Svcs
● Development and Test Svcs
● Email Svcs
● App Infrastructure Svcs
● Storage Svcs
● Backup and Recovery Svcs
● Managed Print Svcs
● Public Key Infrastructure Svcs
• Data Center Facility Svcs
• Data Center DR Svcs
Chief Information Security Officer
Network Services Manager
● Voice Svcs
● Video Conferencing Svcs
● Video Streaming and Archiving Svcs
● Wireless Network Access Svcs
● Third-Party Network Access Svcs
● New Site Installation Svcs
● Data Network Svcs
● Network Security Svcs
● External DNS Mgmt Svcs
● IP Address Mgmt Svcs
● Domain Name Mgmt Svcs
● Unified Comm Svcs
● Mobile Device Support Svcs
● Remote Access Svcs
● Mobility Infrastructure Svcs
Chief Technology Architect
End User Services Manager
● Desktop Computing Svcs
● Core Software Svcs
● County Retained Assets Svcs
● Catalog Svcs
● Network Printer Svcs
● Enterprise File Synchronization and Sharing Svcs
Service Desk Manager
● Service Desk Svcs
● Operations Mgr
● Supervisors
- Shift Leads
- Tier 1 Agents
- Remote Desktop Support Agents (Tier 1.5)
- Training Analysts
- Quality Anlaysts
- Reporting Analysts
- Workforce Analysts
- Knowledge Mgmt Analysts
Deputy Account Executive
Project Mgmt Office Manager
● Project Mgmt Svcs
Business Analyst Svcs Center Mgr
● Business Analyst Svcs
Applications Development Service Manager
● Apps Development Svcs
● Apps Common Svcs
Apps Maint./ Operations Svcs Manager
● Apps Maintenance and Operations Svcs
Transition Services Manager
Contracts Manager
● Contract and Acquisition Mgmt Svcs
Technology Office Manager
● Architecture Svcs
● Integration and Testing Svcs
• Engineering Svcs
Legend
● Cross-Functional Svcs Framework
● Service Desk Svcs Framework
● End User Svcs Framework
● Network Svcs Framework
● Data Center Svcs Framework
● Application Svcs Framework
058 CA CoSD

*The above org chart does not reflect the following positions EAA and Innovation Officer

Centers of Excellence

Geographic deployment of resources at a role level

The Contractor team shall provide services from mainly five (5) locations: County of San Diego; Pontiac, Michigan; Tulsa, Oklahoma, Colorado Springs, Colorado, and El Paso, Texas, with a few individual support personnel at various sites within the United States (individuals who work from home). These sites shall house staff, equipment, and services needed to respond to inquiries over the telephone and by fax, email, and web-based media including web forms. Contractor shall provide support 24x7x365. The following table lists the percentages of services provided from each location.

Service Frameworks

LOCATION	SERVICE DESK SERVICES	END-USER SERVICES	NETWORK SERVICES	DATA CENTER SERVICES	APPLICATION SERVICES
County of San Diego	20%	100%	80%	10%	75%
Pontiac, MI	80%			5%	5%
El Paso, TX					10%
Tulsa, OK			10%	65%	
Colorado Springs, CO				5%	
Other resources			10%	15%	10%

Project Staff Selection and Replacement

Selection and replacement procedures for the project staff

Contractor’s process for selection of personnel to support the County under this Agreement shall be as follows:

- Available positions are announced to the existing team
  - If a current employee is qualified and interested, they may post for the position
- Positions are posted on Contractor’s websites and on Smart Buy
- Interested Contractor, third parties, and external candidates may apply
- Normal hiring process includes interviews by the account team to determine technical competency and fit within the account dynamic.

As relates to the County’s request to maintain specific staffing assignments:

If a Contractor employee staffing an assignment under this Agreement requests to move to another position within Contractor’s organization, the account team shall post the position, identify a suitable replacement, notify the County (if this person is County-facing), and develop a cross-training plan so that the new team member is ready to assume the duties on the outgoing employee, making for a smooth transition. Typically, an employee shall remain in his/her position for a minimum of 2 years before applying for other positions. To apply for open positions prior to the minimum time requirement, approval of the employee’s manager is required.

If a Contractor employee staffing an assignment under this Agreement leaves unexpectedly, the account team shall immediately assign a temporary backfill to review in-flight projects and minimize disruption to the County. In parallel, the account team shall post the position, identify a suitable replacement, notify the County (if this person is County-facing), and develop a training plan to make certain that the new team member has the tools necessary to perform the required functions.

Key Positions / Key Personnel

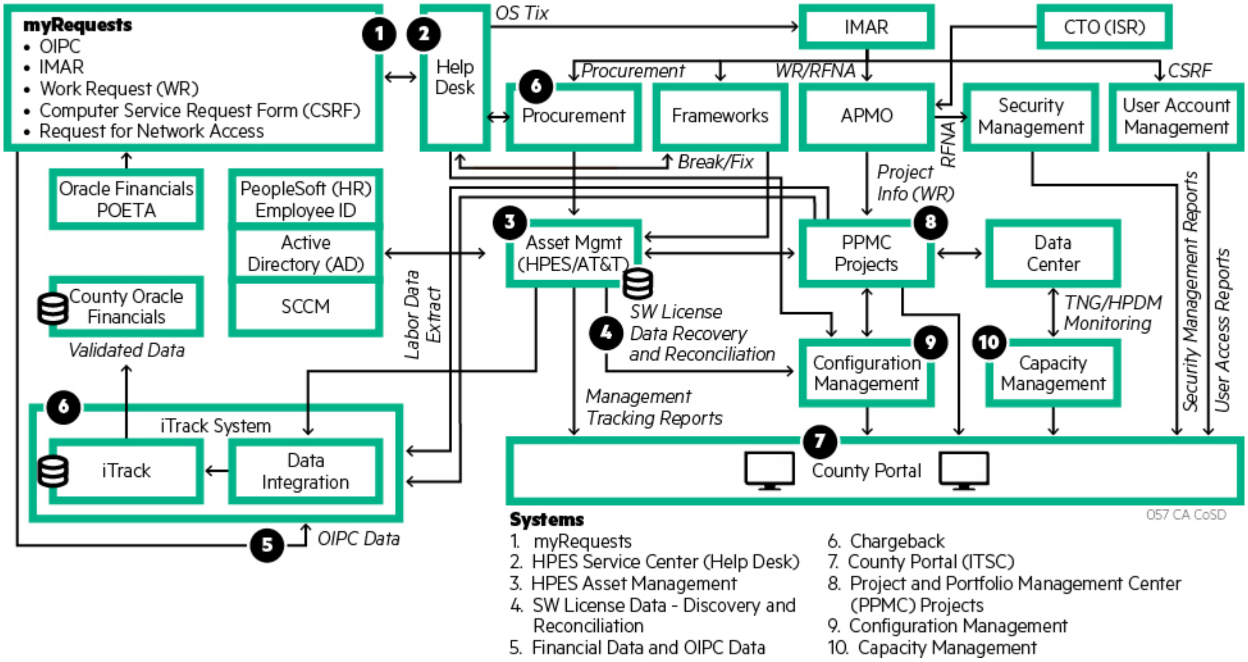
Named Position	Key Positions
Cathy Varner	Account Executive
Laura Floyd	Deputy Account Executive
Kathleen Barghols	Enterprise Service Delivery Manager (SDM)
John Steed	FG3 Service Delivery Manager (SDM)
Frank Krone	CSG Service Delivery Manager (SDM)
Sandra Messina	HHSA Service Delivery Manager (SDM)
Albert Hatcher	PSG Service Delivery Manager (SDM)
David Pugh	LUEG Service Delivery Manager (SDM)
Max Pinna	Contracts Manager
Marcelo Peredo	Chief Information Security Officer (CISO)
Thif Iruthayarajah	Chief Technology Architect (CTA)
Jayaprakash Boreddy	Enterprise Application Architect (EAA)
Mark Morin	Cross Functional Services Manager
Curtis Yancey	Service Desk Manager
Hector Vaquedano	End User Services Manager
Jeff Williams	Network Services Manager
Michael Boscarino	Data Center Services Manager
Tina Terlecki	Application Maintenance and Operations Services Manager
Mark Roehr	Applications Development Services Manager
Nelson Diaz	Project Management Office (PMO) Manager
Chris Spanka	Transition Services Manager
<TBD>	Innovation Officer

2. Cross Functional Services

2.1. Overview

Contractor shall reliably manage the County's IT environment through a consistent and standardized Cross Functional Services model, illustrated in the figure below.

Contractor Cross-Functional Services Model



Delivering centrally managed, cross-functional uniformity of County cross-functional IT services.

Contractor's Information Technology Infrastructure Library (ITIL)-aligned service management practices shall support all Contractor-delivered IT services, making certain that its service delivery meets or exceeds County requirements and expectations. Contractor shall employ industry best practices, processes, and methodologies, optimally combining people and technology to fulfill the County's IT objectives. Contractor shall coordinate and collaborate with County leadership, limiting or preventing misunderstanding and miscommunication through full and open transparency.

Service Now is also under review as an alternate solution for the Standard Reference Architecture (SRA) stack and its functionality. Details of the specific tool used shall be discussed and documented to prepare a notice of decision (NOD) during Transition planning.

2.3. Contract and Acquisition Management Services

2.3.1. Process and Procedures

Contract and Acquisition Management

- Description of solution to meet the requirements

Solution: The Contractor solution shall include an experienced, full-time contracts manager to serve as the single point of contact for the County on all contractual matters, including subcontracts and third-party vendor relationships. Responsibilities shall encompass all contractual issues between Contractor and the County, including contract interpretation, service requests, estimates and pricing discussions, and contract changes and disputes.

The contracts manager shall establish contractor oversight responsibility and provide recurring status reports to the County contracts manager on contractual matters and shall work with County counterparts to respond to unscheduled requests for information. In addition, the contracts manager shall interact with subcontractors and vendors to audit and verify the timely provision of the requested services.

Contractor’s contract management activities shall build performance evaluative criteria to assist the County contracts manager in determining compliance with the Agreement.

- Deployment plan for resources and use of facilities

The Contractor’s contracts manager shall oversee the delivery of the contract management services. The contracts manager shall be knowledgeable about the County’s business and services. A subcontracts manager, procurement specialists, and Contractor’s Global Procurement organization shall provide acquisition management. The contracts manager shall be co-located in the County Technology Office, with a satellite office in Rancho Bernardo.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor’s methodology shall include performance-based management and includes periodic assessments of Contractor’s key performance indicators (KPIs). Contractor shall continually assess these indicators to identify negative trend lines. Contractor shall conduct root cause analysis, where necessary, and take appropriate remediation steps to improve the KPIs and positively influence performance trends—thereby facilitating year-to-year continuous improvement.

Adherence to County procurement policies and procedures when engaging, selecting, and contracting with Third-Parties, including ensuring pricing is fair and reasonable.

Contractor’s Global Procurement organization shall be responsible for making certain that all procurements corporate-wide are performed in accordance with all federal, state, and local laws and policies and that goods and services are purchased at fair and reasonable prices. Contractor’s procurement team shall maintain active and historical records of trusted and vetted third-party vendors from whom Contractor solicits proposals and/or quotations for County goods and services. Additionally, Contractor shall verify that goods and services provided were delivered in accordance with Agreement requirements and County expectations. Moreover, Contractor’s sourcing and procurement team shall flow down all relevant terms and conditions to third parties to verify that all of the County’s requirements are met.

Approach for conducting market scans to purchase Assets from Third-Parties.

The Contractor procurement team shall submit requests for quotations (RFQs) to a subset of vendors identified by Global Procurement as best-in-class providers in their database-based Dunn and Bradstreet (D&B) ratings and other factors as a starting point. Contractor shall continually update this database of vendors to provide a large pool of vendors who offer competitively priced goods and services. Contractor shall use the County – Vendor and Product Assessment Process for vendor and product assessment projects requests. Additionally, Contractor’s account subject matter experts (SMEs) shall assist in market scans by attending conferences and staying abreast of the latest technologies and products and making the Contractor procurement team aware of them. Contractor’s procurement specialists shall work closely with County personnel to make certain that Contractor captures and understands their needs. Contractor shall routinely follow up with them to verify their ongoing satisfaction.

Management, maintenance and publication of the Optional Item Catalog (OIC).

The Contractor desktop catalog manager shall be responsible for managing, maintaining, and publishing the OIC. Contractor shall publish and manage the OIC via the Contractor Service Portal.

Contractor shall issue quarterly requests for quotation (RFQs) for the entire hardware catalog to multiple top-tier suppliers. Contractor shall publish the lowest price obtained for each item in the OIC. If an item is not available during the 3-month period from the low-price vendor, then Contractor shall notify the County and request permission to purchase at the current price.

End-Users shall place acquisition requests through the Service Portal for acquisition of items from the OIC.

Relationships and existing agreements Contractor has with Third-Party developers of government and commercial software products, and how these can be leveraged and accessed by the County.

Contractor has negotiated master service agreements and strategic alliances with a number of IT and enterprise solution vendors, such as Oracle, EMC, Microsoft, Palo Alto, and so forth. Where these negotiated master service agreements and strategic alliances provide expedited access for technical support specific to the third-party vendor's product or software ("reach-back"), Contractor shall provide reach-forward and reach-back to leverage the Contractor leveraged organization for on demand technical support and services. Contractor shall contract with third-party developers on behalf of the County to use Contractor's volume discounts, terms, and conditions.

Managing the County's Desktop Applications Directory (DAD)

After the review team approves the addition to the OIC Catalog for new Desktop Applications Directory (DAD) software, then the Contractor's desktop catalog manager shall add the software to the OIC Catalog (updates to Service Portal OIC Catalog are posted on the 20th of each month). This shall include purchasing software, verifying County-owned software, and transferring software requests to Desktop Engineering. After this is complete and the software is posted to the OIC, the Contractor's desktop catalog manager shall take the licensing documentation and input the data into Contractor's asset database as new DAD entry(ies) updating the Asset Management Database. To manage the DAD item volume, Contractor shall periodically produce and review with the County a report showing the last order date of all DAD items, as well as the number of instances installed. Contractor shall remove items from the DAD that are no longer being ordered to remain within the DAD limits.

Description of how hand off and touch points are managed to be seamless to the County End-User requesting the Service (e.g., Contract Management Services, Applications M&O Services, Applications Development Services, Service Desk Services, Network Services)

Contractor, in cooperation with County stakeholders, shall maintain policies, procedures, and best practices to enable the seamless provision of IT services as projects or service requests transition from point to point through instantiation or implementation.

When the End-User requests a project, then he or she shall fill out a form with the required fields and a Statement of Work (SOW) describing what he or she is trying to accomplish. After the service request form is finished and approved by the County, then the request shall be sent to Contractor as a request for a Budgetary Estimate (BE). The Contractor PM and technical team shall prepare the BE with scope, requirements, assumptions, and a cost estimate for the requested work. Once approved, the project shall proceed to the scope execution phase. Changes in scope shall be evaluated within the change management review and approval process. After the scope is completed, the project shall be formally closed down. The Contractor PM shall prepare a Project Closure

Agreement (PCA), and the Contractor project support office (PSO) shall send it to the County for approval. If not approved, the Project Closure Agreement shall be sent to the Contractor PM for updates and then returned to CTO Contracts for approval. If approved, the project shall be officially closed, and the data in the PCA shall be legacy data for the project. These Contractor and County tailored policies and best practices shall be continually refined to minimize End-User impact and disruption—enabling seamless implementation of the requested services.

Evaluating security to ensure the County is aware of the risks or issues in cloud-related services to enable the County to make an informed decision based on Contractor recommendations.

To provide adequate evaluation of risks and issues in cloud-related services, Contractor shall follow the County Cloud Service Provider Request procedures, as well as Contractor's Global Procurement organization's cloud service provider review process. The Contractor Global Procurement processes shall include reviews of liability, data protection and security, termination rights, location of services, location of jurisdiction of services, control/visibility of subcontracting, rights to suspend service, and unilateral/provider amendments to service features. Contractor shall develop policies, architectures, and solutions necessary to facilitate confidentiality, integrity, and availability of the County's data and systems. Contractor shall analyze evolving County architectural landscapes along with security and privacy controls, backup and continuity requirements, and user access and permissions. In addition, Contractor shall factor these and other considerations into its cloud recommendations and governance guidance for presentation to the County. Contractor shall apply the right level of logical and physical monitoring and management of County data center operations and cloud-based assets.

Contractor's security experts shall be well versed in cloud selection, migration considerations, and End-User accessibility as well as denial of service to unauthorized or outside sources. Contractor shall closely monitor these operations to facilitate strict security compliance and security risk mitigation.

2.4. Integrated Asset Management Services

2.4.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall provide an Integrated Asset Management System (IAMS) that reduces the amount of manual intervention required to verify, check, and fulfill requests while adhering to governing policies and standards.

It is important that Contractor answer five fundamental questions to demonstrate the scope and dimensions of effective asset management:

- What do you have?
- Where is it?
- How well is it working?
- How much does it cost?
- How well does it support your business?

IT asset management (ITAM) shall address these questions by providing processes, tools, data, and people across the entire life cycle. ITAM shall manage the legal obligations associated with vendor warranties and support commitments, entitlements, and asset disposal.

Contractor's solution is based on an upgrade to HPE's Asset Manager from Asset Center. Asset Manager influences IT operations and decision making in the following ways:

- Aligns services to their supporting assets and contracts
- Effectively manages contracts, license agreements, and warranties

- Streamlines the fulfillment of goods and service requests from the service catalog
- Effects complete asset and project audit tracking
- Proactively identifies license compliance issues
- Evaluates opportunities on license maintenance
- Reharvests and reallocates unused software licenses.

As demonstrated in the table below, benefits to the County include productivity, cost control, and risk mitigation.

Benefits Provided to the County

	PRODUCTIVITY	COST CONTROL	RISK MITIGATION
Hardware Asset Management	• Centralizes information and reporting to give the County a "single source of truth." • Organizes required data and provide reporting for compliance with privacy, security, and environmental regulations. Minimizes the risk of noncompliance with software contracts and auditing costs and potential penalties. • Improves asset repository accuracy by highlighting any unauthorized install, move, add, removal (IMAR) to assets.	• Maximizes use of existing hardware assets across the enterprise	
Software Asset Management	• Centralizes information and reporting to give the County a single source of truth.	• Maximizes use of existing software assets across the enterprise • Verifies the number of licenses in use and determines future licensing requirements based on business demands. • Assists in maintaining compliance with license agreements.	• Assists in detecting unauthorized software and enforces software restriction policies relating allowable software that is allowed to run in the County environment.
Hardware Logistics	• Provides reliable system integration facilitating correct configuration and staging of new and replacement devices so that employees are up and running with minimal downtime.		

- Deployment plan for resources and use of facilities

The following resources are required to implement the Contractor solution:

- IT asset manager
- IT SW asset manager

- Warehouse lead
- End-User HW asset analysts
- End-User SW asset analysts
- Server SW asset analysts.

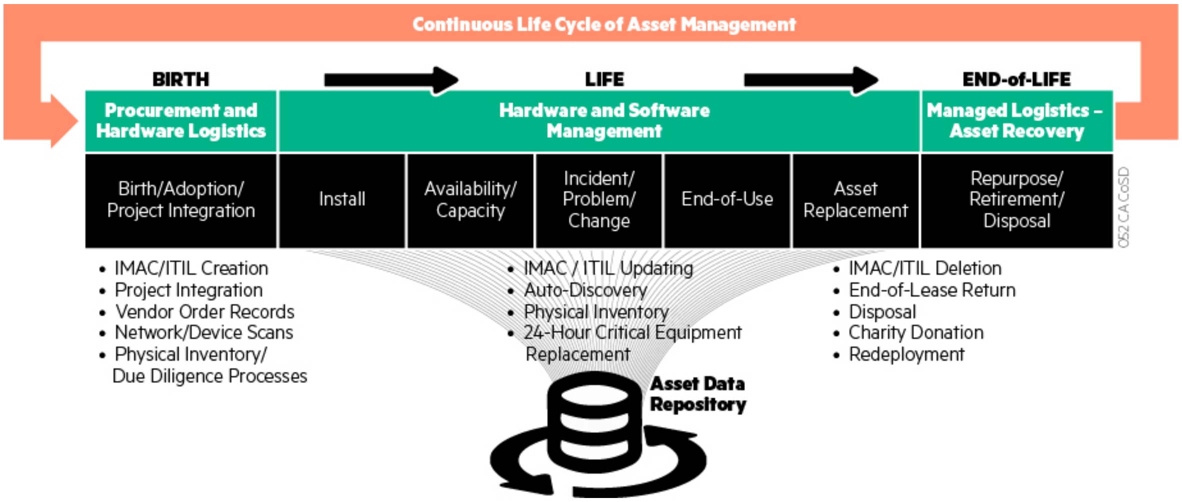
The IT asset manager and warehouse lead shall operate from the Contractor's Rancho Bernardo facility. Contractor shall also leverage resources located at its Tulsa data center the asset management team shall process assets into Asset Manager and provide site support technicians based out of the Rancho Bernardo facility during IMARs, break-fix, and refresh projects for deployed desktop assets.

Contractor shall use a facility approach for stocking the asset inventory, employing two levels of warehouse stocking to speed delivery of equipment in support of IMARs and refresh, while mitigating both inventory and manufacturer disruption risks. County-specific inventory shall be held first at the Contractor's Rancho Bernardo facility and secondly at its partner locations.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor's asset management process shall track all facets of IT assets, from request (procurement) to problems or changes to the asset during its useful life, to disposal (end of life). The life cycle of County asset process is depicted in the figure below.

Contractor Asset Life Cycle Management Process



Providing complete visibility of all County assets throughout their entire life cycle.

Hardware Asset Management

Hardware asset management shall include asset tracking and lease contracts, providing an asset repository that includes records of all hardware assets. Contractor shall track, report on, and analyze the assets from the asset repository.

By tracking assets through the asset repository (database) using various methods and toolsets, Contractor shall capture and report the asset configuration information at the device level (for example, desktop, network, and server). Contractor shall manage the accuracy of the information through cross-checks with other systems and through process links from other services such as Service Desk, site support, and workplace server management services.

The table below identifies the County's high-level deliverables for hardware asset tracking.

High-level Deliverables

DELIVERABLE	ACTION
Asset Repository	• Populates the asset repository with inventory records established during implementation
Asset Record Creation	• Ongoing – as new assets are procured, records are created and added to the asset repository
Asset Tracking	• Updates asset records in repository to reflect the IMAR work process while it takes place • For servers, a discovery tool remotely accesses devices and provides a channel for validating asset records • Reviews and resolves conflicts or exceptions and mediates them in the asset inventory
Reporting	• Creates standard reports documenting the current inventory • Documents inventory asset data elements specified in the table below • Documents data elements for assets that have gone through IMAR or other change processes • Records and reports on listings of noted discontinued hardware
Monthly Evaluation of Asset Accuracy	• Performs audits on approximately 10 percent of the in-scope asset records to confirm continued asset accuracy • Uses various tools to cross-check accuracy of asset data and records
Asset Exceptions Review and Resolution	• Identifies and remediates exceptions

Hardware Lease Contract Tracking

Contractor’s lease contract tracking increases awareness of all applicable hardware lease agreements for the hardware assets including desktop, midrange, and mainframe platforms provided as a Service. This service synthesizes basic asset data with information from leasing company sources to enable tracking of all assets under lease and of those that are imminently scheduled for lease expiration.

Maintenance Contract Tracking

Through this service feature, Contractor shall compile data and aggregate it into reports detailing the general contract terms for all Assets covered under warranty, including scheduled contract expirations. From this data, Contractor shall prepare a monthly expiration report highlighting potential renewal or replacement actions.

Contractor shall track maintenance contracts to produce the following benefits:

- Provides a single database for easy access to all warranty and maintenance contracts
- Fully uses warranty and maintenance contracts and avoids expenditures for costly third-party maintenance
- Ensures ongoing warranty and maintenance coverage, where applicable.

Data collected for Warranty and Maintenance Contract Tracking and Lease Tracking is shown in the table below.

Data Collected

FIELD NAME	FIELD DESCRIPTION
End Date	Lease or maintenance contract end date

FIELD NAME	FIELD DESCRIPTION
Expiration Date	Warranty end date
External Reference Number	External reference number (contract number)
Maintenance Contract	Number of maintenance contracts associated with an asset
Purpose	Purpose of contract
Start Date	Contract start date for lease or maintenance

Software Asset Management

Contractor shall provide software asset management to effectively manage, control, and protect the licensed software assets throughout their life cycle. Coverage shall include all in-scope desktop, midrange, and mainframe software that meets registration requirements and has the base data fields required for tracking. This includes both Desktop Applications Directory and Portfolio Applications.

Contractor shall employ standard processes to track and maintain records for:

- Auto-discovered software found during environment scans
- Any transferable details from prior hardware asset tracking discovery
- COTS applications
- Contractor-procured, -owned, and -managed COTS software, as applicable
- County-retained and Contractor-managed COTS software

Software asset management shall include the following services for in-scope software publishers and titles:

- Software license entitlement reporting
- Software installation reporting
- Software license and maintenance tracking
- License compliance management services

Software asset management for desktop and Portfolio Applications shall follow the same high-level lifecycle processes. Creation of the asset record in the IAMS shall occur upon purchase and receipt of the software. The attributes of the assets and associated procurement transactions (ex. vendor, products, license metric, quantity, term, acquisition date) shall be populated in the system and represent the entitlement. Installation records in the IAMS shall be created either through automated discovery or direct entry into the IAMS. Updates to asset records shall be made to reflect IMARs as required.

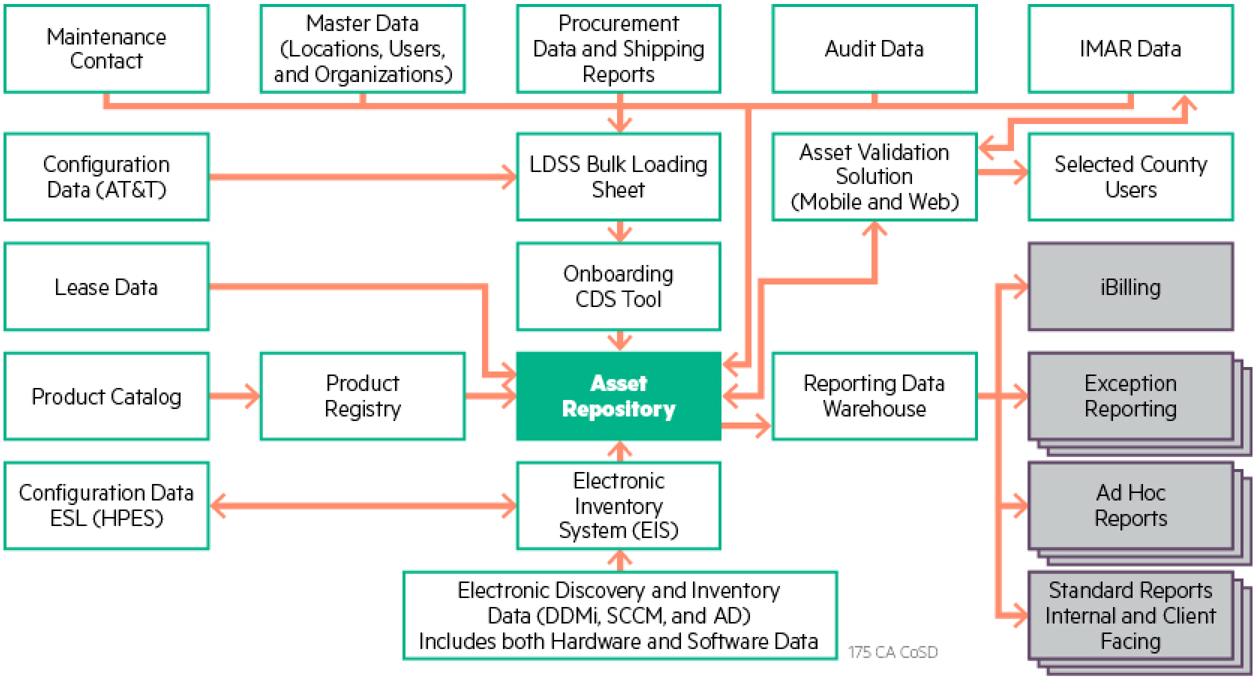
As part of software asset management, Contractor shall maximize use of existing assets through re-harvesting and reallocation of existing software licenses. When there is a requirement for additional software licenses, Contractor shall check whether the current entitlement quantity exceeds the current quantity consumed and, if so, uses the excess licenses to fulfill the requirement. Contractor shall also facilitate workstation/End-User license transfers. Licenses assigned to employees who have left the County shall be reassigned to new hires; also, existing licenses may, from time to time, be reallocated to employees with a current need for that application.

Asset Retirement/Charitable Donation

For retired personal computers, laptop computers, tablets, and associated peripheral assets that were used by the County, Contractor shall donate these assets to the San Diego Futures Foundation (SDFF), at no additional cost to the County.

The figure below depicts Contractor's IAMS. It receives data updates from the Contractor's configuration management database (CMDB), the AT&T CMDB, auto-discovery and inventory tools such as HPE's Discovery and Dependency Mapping Inventory (DDMI), System Center Configuration Manager (SCCM), and Active Directory) as well as bulk load updates and manual updates by asset analysts. Asset data in the IAMS shall be viewable by approved County personnel using the Asset Validation System (AVS) tool, which has a link on the Service Portal.

Contractor Integrated Asset Management System


Maintenance Contact
Master Data (Locations, Users, and Organizations)
Procurement Data and Shipping Reports
Audit Data
IMAR Data
Configuration Data (AT&T)
LDSS Bulk Loading Sheet
Asset Validation Solution (Mobile and Web)
Selected County Users
Lease Data
Onboarding CDS Tool
iBilling
Product Catalog
Product Registry
Asset Repository
Reporting Data Warehouse
Exception Reporting
Configuration Data ESL (HPES)
Electronic Inventory System (EIS)
Ad Hoc Reports
Electronic Discovery and Inventory Data (DDMi, SCCM, and AD) Includes both Hardware and Software Data
Standard Reports Internal and Client Facing
175 CA CoSD

Automated system to facilitate transparency and accuracy of all software and hardware assets.

Approach to ensure that all Assets Contractor procures for the County are procured in the most cost-effective manner possible, so that the potential reacquisition of such Assets by the County in the event of a disentanglement is favorable to the County.

Contractor's account team shall provide dedicated support from the Contractor's leveraged supply chain practice to source all products and services to ensure Contractor provides the best value for the County. This resource shall be fully aware of Contractor's product needs, shall have leveraged contacts with all Contractor OEM providers, and shall assist Contractor in procuring items in a competitive format.

Contractor shall employ an economic order quantity model to make sure that it is holding the minimum required inventory to be deployed to the County in the case of a disentanglement while still meeting the required refresh and IMAR commitments. This shall include:

- Contractor stocking a supply of desktop and laptop RU hardware units in the Rancho Bernardo warehouse against a 6-month rolling forecast based on the customer-agreed refresh plan and a buffer against IMAR estimates.
- To lessen production disruptions, maintaining agreements with Contractor's value added resellers (VARs) to hold additional supplies of County-specific configured assets in their warehouses.

Integrated Asset Management systems and procedures

The Contractor solution for Integrated Asset Management is based on Contractor's toolset called Standard Reference Architecture (SRA). Integrated Asset Management is a component within SRA. The core software application and repository used for Integrated Asset Management is Asset Manager.

Updates to the SRA toolset shall be made available on a regular basis. Contractor shall conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that Contractor is using the right technology to support the County's needs and remain in supported status.

The primary interfaces into Asset Manager shall include direct use of the client software application, the Load Data Spreadsheet (LDSS) tool for bulk loading of data from spreadsheets, and the Electronic Inventory System (EIS) for electronic discovery data.

The following list contains the Integrated Asset Management systems, data sources, and their integrations:

- **Configuration Data (Contractor)** – ITIL-based Configuration Item (CI) data and Asset Management data shall be integrated. The tool used to manage CI data (ESL) shall be integrated with the tool used for Asset Management data (Asset Manager). Changes in CI data shall be passed to Asset Manager via the EIS system. EIS shall also handle integration of discovery tools including DDMI, SCCM, and Active Directory.
- **Configuration Data (AT&T)** – AT&T configuration data shall be integrated with Asset Manager via the LDSS interface.
- **Product Catalog –**. Contractor shall update the product catalog on a regular basis. It can also be updated with County specific applications. The product catalog shall allow users of Asset Manager to work with a normalized set of asset names.
- **Lease Data** – For those assets that Contractor leases, lease contract data is entered directly into Asset Manager's Contract Module as "lease contracts." Assets are associated with the lease contract under which they were acquired.
- **Maintenance Contracts** – The management of maintenance contracts shall be a standard feature of Asset Manager. Contract data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **Master Data –** Master data, such as County locations, shall initially be loaded via the LDSS bulk load tool and maintained on an ongoing basis via the client software application.
- **Procurement Data** – Tracking procurement data for assets shall be a standard feature of Asset Manager. Procurement data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool upon receipt of the assets.
- **Audit Data –** Tracking audits of assets shall be a standard feature of Asset Manager. Audit data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **IMAR Data** – Updating assets in response to IMAR changes (ex. an asset move) shall be performed via the client software application, LDSS bulk load too, or Asset Validation Solution (AVS), described below. AVS shall allow field technicians to directly update Asset Manager in the field.
- **IBilling** – Exports of asset data from Asset Manager shall be imported by the IBilling system for the purposed of billing asset-based Resource Units**.**
- **Reporting** – As part of the SRA toolset, a Reporting data warehouse shall provide support for standard reports, ad hoc reports, and exception reporting.

Contractor's IAMS, described above, shall be accessible to the County. Contractor shall provide a subset of the County manager's direct access to asset manager data using the AVS via the Service Portal. AVS is a web user interface directly reading live asset data.

Ongoing management of the Asset inventory and configuration data.

The Contractor’s IAMS shall receive feeds from DDMI (auto-discovery for server) and SCCM and AD (desktop) and be compared to the CMDB and asset repository for accuracy. Asset records shall be updated to reflect that data as necessary, and reports shall be provided to be actioned against when an asset has not been discovered after a set period of time.

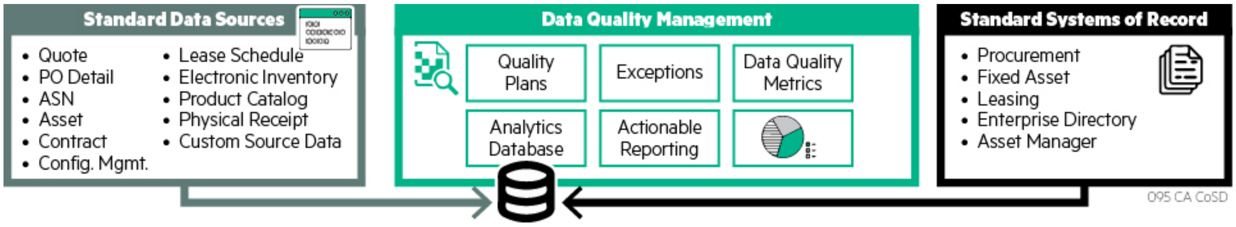
All changes to CI's shall be managed through Contractor’s ITIL-based change management process. No changes to assets shall be allowed unless previously approved.

Contractor’s CMDB (Enterprise System List - ESL) and Asset Manager shall be housed in a secure, U.S-based network segment on the Contractor’s internal network that houses only State and local government data.

Additionally, a comprehensive review of IMAR tickets and refresh project updates shall be undertaken at the beginning of the billing cycle to make sure the asset data is accurately reflected in the files submitted to the iTrack system.

Contractor shall use a data quality management process to validate the accuracy of data in Contractor’s database. That process is shown in the figure below.

Data Quality Management Process



Proven process to ensure the integrity of all Asset Management Data.

Contractor shall validate asset accuracy through the following processes:

- Electronic Discovery – validate Asset Manager assets against assets discovered/active as reported in SCCM, DDMI, AD, and SEP.
- Lease Comparison – HP Financial Services asset lease database is compared to Asset Manager.
- Contractor Fixed/Leased Audit – a randomly selected asset sample is validated via auto-discovery or, if required, manual inventory.
- IMAR – Support technicians validate assets when working on machines.
- Onsite Refresh Pre-Field Inspections – desktop and laptop asset data is validated one month prior to a scheduled refresh.
- Contractor Data Center Asset IMACD processes – all parent assets have an affixed RFID tag, which is scanned as the asset enters or leaves the data center floor, updates are passed to ESL, which updates Asset Manager.

Integration of all asset repositories across the Service Frameworks.

The system shall integrate across service frameworks starting with the HPE Asset Manager asset repository containing and receiving updates to:

- Physical servers

- Virtual servers
- Storage frames
- Network appliances
- Discoverable server software
- Desktops
- Laptops
- Workstations
- Tablets
- Network printers
- Discoverable End-User asset software
- AT&T managed network devices

Updates to this data shall be made via bulk loads (for example, refresh projects, move projects, new assets), nightly feeds of Contractor's CMDB data (ESL), AT&T data, auto-discovery and inventory data, and manual updates as requested by service manager tickets submitted to the asset management queue (for example, IMARs).

Integrated reporting across Assets to show useful information relating to departments, hardware, software, licenses, versions, etc.

Deployed and billable server and End-User data shall be pushed to iTrack on a monthly basis. In addition, Contractor shall upload monthly Schedule 5 reports to the Service Portal. These shall include, but are not limited to, the following reports:

- End-User status changes, deployed End-User assets, static access assets report
- Monthly report of installed End-User software titles
- Monthly End-User refresh report

Contractor shall deploy Enterprise Services Asset Analytics (ESAA) data analysis and statistical reporting engine as part of the SRA toolset. This tool shall analyze data stored in Asset Manager and generate standardized reports for analysis and action including the following:

- Asset record completeness (against pre-defined fields)
- Discoverable devices not discovered
- Discovered devices not showing in Active status
- Assets reaching end-of-life
- Devices approaching end-of-lease
- Devices updated in the last month
- Counts of tracked installed software titles versus entitlement counts

Reports shall be provided to the appropriate desktop or server personnel for research, corrective action, and data updates to the source systems if needed.

2.5. Billing Management Services

2.5.1. Process and Procedures

- Description of solution to meet the requirements

The County chargeback application, iTrack, combined with the Contractor billing data consolidation application (IBilling), shall comprise the tools and associated processes for Billing Management.

The iTrack End-User community, County CTO team, and Contractor have identified specific opportunities for incremental improvements. As an example, managing and communicating County low org changes has been a focus area. Contractor is increasing the integration between IBilling and iTrack in support of improved Low Org management by enhancing IBilling to use Low Org data directly from iTrack for data validation. Additional enhancements that Contractor plans to pursue with the County include integration with PeopleSoft HR for employee-related chargeback data and general chargeback data normalization.

- Deployment plan for resources and use of facilities

Contractor shall use the following resources for its billing management services:

- **Billing Manager** – Responsible for the successful delivery of all billing management services
- **Billing Team** – Technical resources to support the IBilling application and the Framework owners responsible for providing monthly billing data and responding to billing disputes.

The billing manager shall be based in the Contractor's Rancho Bernardo facilities.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's methodology shall include performance-based management as well as periodic assessments of Contractor's Key Performance Indicators (KPIs). As an integral component of Contractor's quality assurance management program, Contractor shall continually assess these KPIs to identify negative trends. Contractor shall conduct root-cause analyses where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, facilitating year-over-year continuous improvement.

- Automated systems and tools involved in solution

Contractor shall use the following tools in support of billing management:

- IBilling: Contractor's billing data consolidation application based on SQL Server and SQL Server Integration Services (SSIS).
- iTrack: The County's customized implementation of Nicus' M-PWR commercial off-the-shelf (COTS) chargeback application
- Billing Source Data Tools:
  - AssetManager
  - ServiceManager
  - PPMC
  - Active Directory
  - myRequests (myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in Transition Services Framework)
  - AppsManager
  - CSRFs
  - Service Requests

Approach to coordinate and reconcile detailed billings and usage on a monthly basis.

The Contractor billing team shall collect input data from the authoritative source systems by the 5th day of each month for each framework: Application Services, End-User Services, Network Services, Data Center, Cross Functional Services, Special Requirements, Catalog Items, and Other. During this initial data collection phase, framework owners shall review both summary reports and rule-based exception reports to verify data completeness and quality.

Following collection of the framework input data, the data shall be aggregated in a format that can be imported into the County iTrack chargeback system by the IBilling application. IBilling applies rule-based billing logic as well as data lookup from reference systems. Additional summary, trending, and exception reporting shall be performed on the aggregated data.

By the 9th of each month, Contractor shall review a summary invoice with the framework owners, billing team, and account management. Contractor shall explain any variances and, if needed, make corrections in the billing system and rerun the processes.

After Contractor management approval, Contractor shall create an invoice in Excel— “Base Services Invoice”— and deliver it to the CTO and the office of Auditor and Controller (A&C) no later than the 10th of the month.

Interface of Contractor billing system to County iTrack, and billing data transfer the County iTrack

By the 10th of each month, Contractor shall load detailed billing data into iTrack from IBilling, the Contractor billing data consolidation application, using automated Structured Query Language (SQL) scripts.

County staff shall process the data using iTrack and notify their staff that the data is ready for their review. Contractor shall load detailed telecommunication records by the 10th of the month. Contractor shall archive all billing data, including source files, for audit purposes.

Processes to ensure a high level of billing accuracy each month.

The Contractor billing team and framework owners shall research and address anomalies in trending and exceptions to facilitate a closed loop feedback review and continuous improvement. Contractor shall maintain monthly metrics to track responsiveness to County change requests; Contractor shall monitor and remediate these when necessary as part of its ongoing performance-based management methodology.

Billing corrections

The Change Request process in iTrack shall be used to make billing corrections. The County has until the 22nd of each month to create a Change Request in iTrack to dispute a charge or to request a name, location, low org, or other change to a billing record. On the 23rd of each month, the Contractor billing manager shall generate a report from iTrack of all approved Change Requests for that period and shall distribute it to all framework owners. The Contractor billing team shall investigate, correct, adjust, or explain all disputes and corrections by the next billing cycle. Contractor shall make corrections in the source systems to provide accuracy in subsequent billing periods.

Credits and adjustments for disputed charges, once validated, shall appear as a credit in the next billing period.

Contractor’s billing manager shall enter comments in iTrack stating the resolution of each dispute. Contractor shall monitor and follow up on unresolved disputes and track them through closure.

After each billing period, by the 15th of the month, the Contractor billing manager shall compare the Change Requests approved to the latest billing file and shall follow up with framework owners on any differences to verify chargeback billing accuracy.

2.6. Security Management Services

2.6.1. Process and Procedures

- Description of solution to meet the requirements

Contractor's security management shall be comprised of a set of policies and procedures for systematically and quickly reacting to incidents or events that affect the County's information infrastructure, systems, and sensitive data. Contractor shall minimize risk and facilitate continuity of County IT operations by proactively preventing and limiting the impact of security breaches, whether internal or external. Using its expertise and experience, Contractor shall work closely with security counterparts and stakeholders to effectively and efficiently improve County information security. Contractor's solution includes multiple factors that at a minimum include:

- Chief Information Security Officer (CISO)
- Risk management program (framework)
- Evaluation and recommendation for tech controls
- Security governance program/board
- Security and risk management awareness training program
- System categorization for information ownership, classification, accountability and protection
- Incident/threat management and response plan
- Security Information and Event Management (SIEM)
- Continuous improvement

Solution: Contractor's approach to security management shall adhere to the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) and its Special Publication 800 series, which shall act as a guide for delivery and compliance for the protection of systems and providing security services to the County. Overseen by the Contractor CISO, Contractor shall leverage this guidance to methodically assess systems and the organization for gaps and vulnerabilities based on the threat landscape, which may pose a level of risk to the organization.

Contractor shall also use a second approach that coexists with NIST standards, the NSA defense-in-depth model, which emphasizes the use of layers and multiple defense mechanisms across the infrastructure to protect data, systems, networks, and users. In the event that one defensive measure is attacked and exploited, there are additional layers and measures protect the assets.

Additionally, Contractor uses Gartner's Security Process Maturity Model to assess and report the "State of Security" and the progress of various security efforts that contribute to the overall security posture of the County. This model scores areas of security based on scale of 1 to 5 scale—the larger the number, the more mature the security aspect being modeled. Gartner provides a score for "peer" values derived from organizations with similar profiles. This maturity model is useful for comparison over time on how well the County is doing in relation to its peers. Moreover, it provides actionable intelligence for use in Contractor's continuous improvement practices.

The Contractor CISO shall have overall responsibility for all aspects of security (with County CISO). In support of Contractor CISO initiatives, strategies, roadmaps, and transformation, the Security Operations Manager shall be responsible for day-to-day operations and activities.

The following are descriptions of each role and their areas of responsibility:

- IS Security Manager – Responsible for all aspects of compliance, applications security reviews, overall information systems (IS) security, data classification, NIST-based guidance, continuous monitoring of controls, and Security Awareness and Training.

- Security Architect – Responsible for security infrastructure and product roadmaps, strategic participation with other frameworks, establishment of secure zones, and infrastructure security.
- Risk Assessor – Responsible for IS risk assessments, strategic risk guidance, compliance support, vulnerability management support, and vulnerability mitigation support.
- Identity Manager/Analyst – Identity and access management, maintain federated identities, monitors and maintains automated access request workflows, End-User provisioning coordination, monthly IAM reports, yearly attestation process, annual update of IAM plan.
- PKI Administrator – Responsible for use case development in coordination with Security Architect, public key infrastructure (PKI) services delivery, facilitate upkeep of CPS document, manage certificate lifecycle, monthly reporting, PKI inventory, and maintenance of public key certificates.
- Vulnerability Manager – Responsible for continuous scan of the perimeter, vulnerability and risk assessment support, vulnerability mitigation, threat management plan/remediation, application scans, coordinate security operations center (SOC) activities, event log analysis and reporting, intrusion detection system/intrusion prevention system (IDS/IPS) management, data loss prevention support, incident management plan/response/handling, and forensic activities. In the event of a data breach, Contractor shall engage the Security Incident Response Team (SIRT) as necessary to assist in the investigation. This team, in collaboration with the Contractor CISO, shall use its experience and SOC capabilities to ensure that all existing information that aid during a forensic investigation is readily available to authorized individuals. This information shall include log files, SIEM activity, data files, and anything else that may be considered digital evidence. Handling such information must follow proper procedures such as chain of custody and preserving evidence.
- Leveraged SOC – Event log monitoring, single pane of glass, unified threat management, incident response, and IDS/IPS monitoring and analysis.
- AT&T Security – Responsible for providing protection from unauthorized use, access, physical access to County hardware/software (HW/SW), firewall management, event logging, analysis, reporting, IDS/IPS in the communications infrastructure, hardware maintenance, identify and correct single point of failures, architecture and management services, roadmap maintenance for network security services, incident response, data loss prevention support, web content filtering, and hardware maintenance to maximize performance.
- IS Security Officer – Responsible for overall security posture of applications, coordination with application owners, and security documentation.
- HPE Leveraged Services – Forensic services, IDS/IPS service, antivirus services, SIEM services, firewall rule implementation, and PKI support.

- Deployment plan for resources and use of facilities

The Contractor security team shall use multiple locations in support of this Agreement. This team shall work closely with the County CISO, CIO, CTO, and other IT personnel, enabling direct communication and the ability to reach out directly to the Contractor team at any time.

The HPE Rancho Bernardo facility shall be the center of support for Contractor staff assigned to support the County. This facility shall provide centralized meeting spaces for engagements between the County contractors and Contractor personnel. It shall also include test environments, training room, video conferencing, and Contractor executive offices.

HPE Tulsa Data Center shall provide the majority of County IT infrastructure and core IT services, including web, application, DB servers, data storage, and data management.

HPE Orlando data center shall host the leveraged ArcSight SIEM solution from which the county's IT infrastructure is monitored 24x7x365.

HPE Colorado Springs Data Center shall serve as the disaster recovery site for the County IT services.

HPE U.S. Public Sector (USPS) headquarters in Herndon, VA shall serve as the primary location for senior Contractor executives and the Enterprise Security Operations Center (ESOC), a service that monitors the SIEM service.

- Key methodologies and processes in proposed solution including year-to-year continuous improvement

Contractor shall use the NIST CSRC information security tools, practices, standards and guidelines to support the County. The CSRC is the primary source of information for security related standard publications that provide computer/cyber information guidelines, recommendations, and reference materials. In addition, Contractor shall rely on NIST Special Publication 800-53 and 800-37, focusing on the Risk Management Framework (RMF) and the County implementation. The RMF is currently in use by all Federal agencies to comply with FISMA requirements. Contractor understands that the County currently does not have a Federal mandate to comply with FISMA. However, there are some systems in the law enforcement community and healthcare systems that require a proven standard to protect those Federal systems as well as systems that may have interfaces to them. Following is a high-level description of each methodology and key processes that are relevant to the County.

Risk Management Framework – RMF shall be the framework for the County's risk management program and shall provide a standard to measure systems critical to the ever-changing threat landscape in today's County IT infrastructure and systems future hybrid cloud environments. Measuring security controls against an established standard enables best-case resource use and an optimal security posture in which the discovery of vulnerabilities and the time it takes to mitigate them takes as little time as practicable. By following and adhering to the RMF, Contractor is able to minimize potential security oriented exploitation and reduce the risk/impact to the County. The RMF implementation shall continuously look for ways to automate and benefit from technology throughout the duration of the Agreement. The essence of the RMF is its simplicity and its versatility to align and integrate with other frameworks. It employs data visualization technology using dashboards influenced by users and graphical representations to reduce the complexity and improve the accuracy of reporting. The risk-based approach to security control selection and testing provides effective and efficient applicability to the laws and regulations that the County must follow. The steps in the RMF Model are:

- **Step 1: Categorize -** Categorize the information system for ownership, classification, accountability, impact analysis and protection; information is processed, stored, and transmitted by that system.
- **Step 2: Select -** Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on the County's assessment of risk and local conditions.
- **Step 3: Implement -** Implement the security controls and document how the controls are deployed within the information system and environment of operation.
- **Step 4: Assess -** Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly and operating as intended, to meet the security requirements for the enterprise.
- **Step 5: Authorize -** Authorize information system operation based on the risk to the County's operations and assets, individuals, third-party vendors; the County determines acceptable risk.
- **Step 6: Monitor -** Monitor and evaluate selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

The Contractor security services team shall provide the requisite knowledge and understanding of each control to take advantage of the expanded set of security and privacy controls. This facilitates integration with other frameworks and other County groups that may be considering the implementation of cloud-based solutions with other vendors. In addition to managing complexity, the Contractor security team shall leverage the concept of common controls and control inheritance to optimally secure each system in the environment. This results in streamlined operations, testing, and more robust application security in already existing traditional and forthcoming cloud hybrid environments.

The tailored RMF roadmap shall make sure that its transition and evolution is low risk, non-disruptive, adaptive, and flexible to meet County demands, as the adoption of cloud-based and hybrid solutions continue to evolve. Security and the RMF are integral to any new IT initiative and avoid the stigma of "delaying" or "preventing" IT projects from moving forward by making sure every stakeholder is informed, educated, and understands the broader and bigger goal of building IT solutions faster and more secure where all frameworks have win-win paths forward.

As more hybrid cloud-based solutions are introduced to solve business needs, Contractor shall rigorously test and enhance the controls surrounding third-party vendors to minimize risk and avoid delays. Controls designed to monitor ingress and egress of data, data flows, audit and accountability, security monitoring, and many others shall be the focus of Contractor when interacting with third-party vendors.

Defense-in-depth –Contractor shall implement the defense-in-depth approach to goal of delaying the attack and buying time to detect and respond in an effort to mitigate or eliminate the consequences of a breach. Elements of defense-in-depth include antivirus, identity management, biometrics, demilitarized zones, data centric security measures, encryption for data at rest and in transit, firewalls, hashing of passwords, intrusion detection systems, logging of events for auditing, multifactor authentication, vulnerability scanning, physical security, access controls, awareness and training, virtual private networks, sandboxing, intrusion prevention systems, and others.

IT Maturity Model – Contractor and the County use a Gartner IT maturity model that assesses the County's information security program and helps provide recommendations for areas of improvement based on the areas identified. It also provides recommendations, technical and non-technical, to address issues. The results shall be presented to the CIO on a monthly basis or as required.

The security roadmap areas of focus shall include but not be limited to:

- **Governance, Organization and Personnel***:* How the County's information security function is organized and governed, and what the scope of the information security program is. How the County staff organizes its information security function, where it gets support from within, where it is supplemented using third-party service providers, and what areas require investment in training and hiring.
- **Policies, Standards, Procedures and Documentation:** How the County articulates and communicates its policies for information security to the business, and how these policies are supported by clearly defined standards and operational procedures. How the County stores and manages the documentation relevant to its information security environment, including as-is state, in-flight projects, assessments, audit findings, and other related materials.
- **Information Classification:** How the County classifies information and critical systems to determine appropriate information security measures based on the organization's appetite for risk.
- **IT Risk Management and Compliance:** Describes the County's risk posture, and how it assesses whether to accept, transfer, mitigate, or avoid certain risks. How the County manages its responsibilities with respect to legal, regulatory, and audit compliance.
- **Identity Management:** How identity management technologies and processes are used to create and manage identities of the various County constituents (e.g., employees, vendors, contractors, etc.)
- **Runtime Access Control:** Determines what technologies and processes are used to manage permissions and access to the County's networks and applications.
- **Software Development and Testing:** Describes how a security mind-set is integrated with software development life cycles, secure coding practices, outsourced software development, and infrastructure deployments. Describes how systematic testing of code, applications, and infrastructure components is integrated in life cycle processes.

- **Applications and Information Repositories:** How security implications relevant to applications, application development, portals, communication and collaboration platforms, file storage and transfer are reviewed.
- **Encryption:** Describes how the County uses encryption for protecting data in transit, data at rest, strong authentication, and digital signing?
- **Security Awareness and Training***:* How the County communicates the importance of information security to the business at large.
- **Change and Release Management:** How the County controls changes in their hardware, software, and supporting infrastructure while maintaining suitable and appropriate information assurance.
- **Incident Response:** How the County responds and escalates responses during critical security incidents.
- **Threat Response:** How the County responds and escalates responses during critical security threats.
- **Resilience Processes:** How the County implements business continuity management and IT disaster recovery planning and testing to protect the resiliency of its infrastructure.
- **Audit Processes:** How regular internal and external audits verify compliance with corporate policies, standards, and procedures.
- **Network Perimeters and Zones:** Determines what network perimeter mechanisms are used by the County to enforce zone boundaries and protect sites, systems, and users across a distributed infrastructure. How zones of trust used by the County to protect their IT resources on communications networks. How the County detects and responds to security incidents on their network.
- **System Zone Placement:** How the County places systems in security zones.
- **Endpoint Admission:** What approaches the County uses to control client endpoint admission to zones and resources.
- **Host Security:** What management and protection postures the County takes with regard to host system security.
- **Vulnerability and Patch Management:** How the County manages and remediates data, software and configuration vulnerabilities.
- **Anti-Malware:** What mechanisms and approaches the County uses to mitigate malicious software such as viruses, spyware, and Trojan horses.
- **Data Loss Prevention:** What approaches the County uses to prevent the unauthorized exfiltration of company confidential information.
- **Security Information and Event Management:** How the County monitors the network and critical systems, including audits of critical system access and logs.

Methodology to protect the security and confidentiality of data and information that is proprietary to the County or subject to special statutory protection

Contractor shall maintain a robust flexible set of risk-based security methodologies to protect the County's information systems and assets. Contractor shall use the NIST RMF, Defense-in-depth, and the Gartner's IT Maturity Model. Additional guiding principles shall include the minimization of the use, collection, and data protection of what is strictly necessary to accomplish county's business. Contractor shall support the County-classified data each system is processing or storing and appropriately determine the levels of protection based on the data classification and impact to the County. Contractor shall then implement the appropriate levels of safeguards based on the data classification. Additionally, a robust set of processes and procedures shall be in place to handle incidents involving the compromise of the data.

The NIST-based RMF fundamental tenets of security include controls that are specifically designed to protect the confidentiality and integrity of data. At a high level, the controls include the creation of policies and procedures, awareness and training, conducting Privacy Impact Assessments (PIA), identifying and classifying sensitive information, and record retention and disposal of information. Other control specifics include:

- **Access Enforcement** – The County controls access to confidential data through access control policies and access enforcement mechanisms. At the enterprise level, employees are part of role-based Active Directory (AD) groups which are determined using a Change Services Registration Form with approval and consent of a direct employee supervisor. Other non-enterprise systems control access with local management capabilities. As part of the roadmap, a full enterprise identity management capability shall be in place to better secure and manage access controls.

- **Least Privilege** – Contractor shall enforce the most restrictive set of rights and privileges for each End-User in a specific role. For confidential information, Contractor makes sure that users only have access to the minimum about of data needed to perform their job.
- **Auditable Events** – Contractor shall monitor events of systems that contain confidential information and shall make sure there are regular reviews and analysis of system records that indicate inappropriate or unusual activity affecting this data. Investigations shall occur when suspicious activity is detected and violations are reported.
- **Identification and Authentication** – County users shall be uniquely identified and authenticated before accessing confidential information.
- **Media Access** – Contractor shall restrict access to media containing confidential information, often through encryption. Media includes CDs, USB flash drives, backup tapes as well as non-digital media such as paper.
- **Media Transport** – Contractor shall protect digital and non-digital media including confidential data transported outside the organization. A data transfer request process shall be used to scrutinize the data (often encrypted) that leaves County premises.

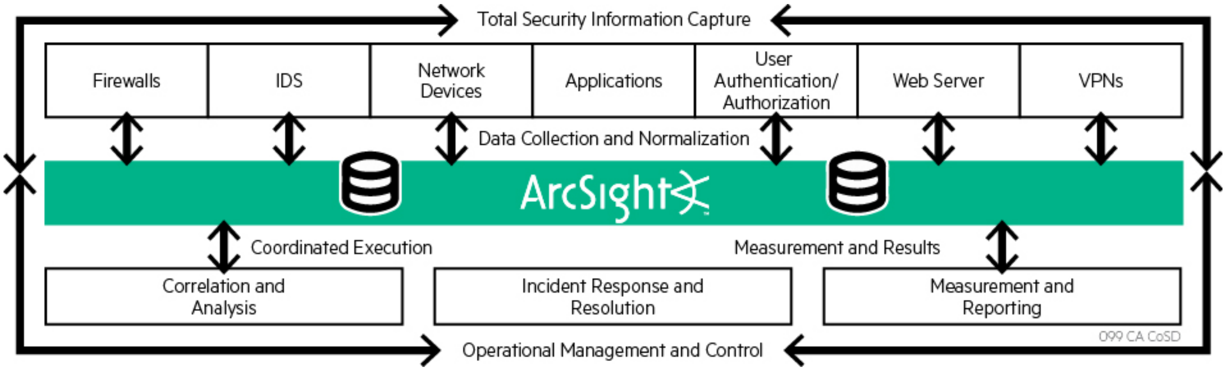
All of these sets of controls shall be implemented at the infrastructure level and on applications that process confidential information. The visibility of how effective controls are being on the lookout for new threats, identifying vulnerabilities, and having a sound mitigation strategy to eliminate or minimize risk results in an optimally protected enterprise.

Approach to data analysis of SIEM information and remediation of identified risks or vulnerabilities.

The major components that comprise the Contractor’s SIEM solution shall be: monitored endpoints that generate security events, security data collection servers that collect and normalize events from disparate endpoints, a security information event manager backend that correlates and analyzes collected events and a web portal that presents processed events and alerts. Finally, the SIEM solution shall include security incident response processes to coordinate analysis and resolution of security issues.

Contractor shall use the ArcSight platform, illustrated in the figure below, to perform the aggregation and correlation of security events generated by different data collection points. Palo Alto logging (traffic, threat, and URL) shall be collected by the Palo Alto centralized managed server platform, Panorama. All SSLVPN logging, as well as DHCP logs shall be gathered by the Juniper JSA device. These two devices shall then forward their logs to both the Contractor’s SIEM (ArcSight) collector, as well as the AT&T managed SOC group. Data center logging (IPS sensors and firewalls) shall also feed to the Contractor SIEM. Contractor shall analyze and resolve issues to provide an additional layer of security. An event alert from either group shall trigger a collective investigation effort between Contractor and AT&T.

ArcSight Platform


Total Security Information Capture
Firewalls
IDS
Network Devices
Applications
User Authentication/ Authorization
Web Server
VPNs
Data Collection and Normalization
ArcSight
Coordinated Execution
Measurement and Results
Correlation and Analysis
Incident Response and Resolution
Measurement and Reporting
099 CA CoSD
Operational Management and Control

The ArcSight Platform provides tool information security capture, coordination, management, and reporting

At a high level, the process to escalate and respond incidents shall be as follows:

- The Contractor security team shall investigate alerts, determine criticality and, if the criticality is severity one or severity two, shall notify the County and Contractor security about the event. If the event does not meet critical criteria, HPEs shall follow the Contractor's internal procedure for noncritical incidents and shall report to the County in the monthly security reports.
- In the event of a severity one or two, Contractor shall initiate the investigation and contact the County CISO and Contractor operations or any support team requested to alert them of the incident per the Severity Escalation Matrix.
- Contractor shall investigate the incident and activate an incident response team (IRT) as needed. If the documented preapproved, incident containment strategy exists to mitigate threat, the IRT shall immediately execute plans to resolve incident.
- The IRT shall determine resolution strategies for County approval. If required, the team shall initiate the change management process by submitting requests for change (RFC).
- The IRT shall execute a containment strategy upon approval of an RFC, if required. The strategy shall include plans for the prevention of further damage caused by the incident and shall be reviewed by the County CISO.
- The IRT shall execute eradication strategies when the RFC is approved and reported to the County CISO.
- The IRT shall execute recovery strategies upon approval of RFC by the County CISO.
- Contractor shall document the incident and close the incident.
- Contractor shall conduct a lessons learned meeting to update strategies, as needed.

Each process of the SIEM incident response shall be included in the yearly review process, which contributes to the maturity of security services. Any areas of improvement or lessons learned shall be incorporated in the updated process and teams shall be aligned accordingly.

Approach to assess the County's security environment.

Contractor shall continuously monitor in real-time mail threats, inbound and outbound network traffic, and discrete data formats in which information leaves County's networks. Additionally, Contractor's ESOC shall respond to any possible threat by investigating whether it is a true incident or if it is a false positive. False positives shall be used to constantly fine tune IPS/IDS and the heuristic engine for data analysis.

Contractor shall conduct vulnerability scans for a maximum of 3,000 IP addresses in the Front DMZ zone as well as the library network. The plan is to increase the number of servers to include all critical servers based on function and data classification they store or process.

Additionally, Contractor shall conduct scans of servers before they go into production, which results in identification of vulnerabilities in servers before they go live. Contractor shall mitigate high and moderate vulnerabilities before any server goes into the production environment.

Contractor shall conduct policy compliance scans on all production servers on a monthly basis. Contractor shall make sure County servers are compliant with Contractor security policies and are up-to-date with patches.

Contractor shall also execute an annual network penetration test restricted to the DMZ. The Contractor network penetration testing process shall include actions that reduce the risk of exposure to the County's most critical online assets and, detailed descriptions for quickly managing or eliminating security exposures. This streamlined, granular approach to risk management enables security policy compliance to become an integral part of the overall security process.

As part of the RMF, Contractor shall document and test environment controls on a predefined efficient schedule. Contractor shall assess the security controls using appropriate procedures to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the County. The ongoing monitoring of security controls in the environment shall also include documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

Contractor and the County CISO shall conduct monthly self-assessment using Gartner's IT Maturity Model and report to the County via CIO briefings. This provides independent validation to the County of Contractor's performance.

Approach to assess the County's application vulnerabilities and security risks, and approach for analyzing and assigning classifications to County Data.

Checklist Based Approach

Contractor shall use an application checklist to identify areas in which the application under review is not compliant with specific security requirements. The application checklist shall be a documented set of questions based on County security policies. The requirements on which the application checklist shall be based are documented in the County Security Management Plan.

The compliance questions shall be categorized into the following security areas:

- Authentication
- Audit
- Nonrepudiation
- Host security
- Enclave
- Access Control
- Confidentiality
- Physical Security
- Application Security
- NIST
- Support
- Integrity
- Network Security
- Data security

Application team members shall respond to an extensive set of questions at different stages of the project, and the list shall then be reviewed by the security team. A scorecard shall then be derived from the questionnaire that shall be rolled up to a dashboard for all applications going through this process. The dashboard facilities identifying trends within specific security categories across multiple applications.

RMF-Based Approach

Applications shall go through the RMF, as described at the beginning of this section. All applicable controls shall be determined by the data classification and take into account factors such as compliance with HIPAA, Privacy, PCI, and other applicable laws and regulations.

Encryption Requirements for Data Security and Protection

Contractor shall provide the following encryption to protect data in transit, at rest, and the PKI Enterprise implementation:

- Data in transit
  - Transport Layer Security (TLS) – Web servers use TLS with digital certificates provided by Entrust.
  - Secure Sockets Layer (SSL) – Web servers use SSL with digital certifications provided by Entrust.
  - Server Message Block (SMB) – Applied to Windows shares (NAS) and files in transit.
  - Virtual Private Networks (VPN) – Junos VPN uses IPsec tunnel. Traffic between the two points is encrypted.
  - Wireless Encryption – Wireless Access Protocol provides encryption on all wireless data exchanges.
  - Email Encryption – TLS to all inbound connections and to trusted outbound domains. Cisco IronPort Office message encryption.to be replaced with Exchange Online Protection (EOP)
  - Mobile Devices – SSL encryption for all communications with County network when using Pulse VPN. Email is encrypted using TLS inbound and outbound when accepted by both parties.

- Data at rest
  - Endpoint Encryption – Symantec Endpoint Encryption provides maximum protection by encrypting each hard drive sector by sector.
  - Database Encryption – Transparent Data Encryption is used in some SQL databases.
  - Removable Media Encryption – Thumb drives ordered from the catalog use AES 256-bit encryption.
  - Password Hashing – New applications or modified during refreshes that store passwords use hashing algorithms to prevent storage in clear text.
  - Mobile Devices – Devices are encrypted using the Operating System default encryption capabilities where appropriate. Additionally, devices shall use a digital certificate to authenticate to AirWatch.

- PKI
  - User Authentication – Symantec Digital Certificates in Active Directory.
  - Device Authentication – Symantec Digital Certificates in all devices.
  - Digital Signature – Self Signed Digital Certificates by ARX and CoSign.
  - Other use cases shall leverage the current Enterprise PKI Symantec solution.

Contractor shall continue to implement solutions with encryption where technology allows for it. Opportunities to improve in this area include technical refreshes and new implementations.

2.7. Service Delivery Management (SDM) Services

2.7.1. Process and Procedures

- Description of solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The Contractor approach shall include repeatable, ITIL compliant, delivery of County IT services that consistently provide high-quality IT service delivery across all frameworks.

Contractor's Service Delivery Management services shall be applied and enforced by its enterprise service delivery manager (ESDM) along with the individual service delivery managers (SDMs) assigned per business group. Contractor shall continue its delivery of these services through proactive communication and collaboration with all affected stakeholders. In addition, Contractor shall provide timely guidance and measure results accordingly as required. Contractor shall document its efforts and make this documentation available on the Service Portal. Contractor shall routinely solicit County and End-User feedback as input into its continuous improvement processes.

Solution: Contractor shall assign a single service delivery manager (SDM) to be the point person for each business group. SDMs shall perform the following, at a minimum:

- Incident management
- Problem management
- Change management
- Release management
- Escalation management/Service Request status
- Communication
- Billing management
- Availability and capacity management
- On-call rotation

The on-call rotation in which the SDMs shall participate is critical to facilitate centralized after-hours support to the County for issue resolution as well as making sure each SDM has appropriate amounts of time off and vacation as required. Contractor shall provide five SDMs who shall rotate on-call every five weeks. During business hours (Monday through Friday 6:00 a.m. to 6:00 p.m.), each SDM shall be responsible for their own business group. After hours and on weekends, the on-call SDM shall take primary responsibility for any issue and works it to resolution. If an enterprise issue emerges during business hours, the on-call SDM shall take point for this issue initially—and possibly to completion, depending on the scope of the issue. If an issue arises during this time within the business group for that on-call SDM that requires their focus and attention, another SDM shall be assigned to take over the new issue. All SDMs from each business group shall be required to work any/all enterprise related issues/disasters that require a shift rotation. The on-call SDM shall verify that the correct customer from the business group is notified and that the SDM assigned to that business group is aware if anything has occurred in their space so they can address it. Problem management is a day-to-day responsibility for the SDMs, and they shall be assigned activities to work whether it be proactively or through tickets, escalations, and so forth. Contractor's enterprise problem manager shall report, track, and communicate all problem management issues worked by the team and the account as required in the weekly CTO Operations meeting. Each SDM shall also report any problems being worked by them through this process that impact their business group or the enterprise in the monthly portfolio review meetings that they shall be required to attend.

For capacity management, each SDM shall be responsible for using report-based findings and data to facilitate the health of their servers and applications for that particular framework. The SDMs shall operate proactively to make certain this health is sustained, reliable, and predictable. They shall work closely with the capacity manager on the account who owns the activities and verifies that Contractor is resolving alerts as well as reviewing trends to implement the right steps to prevent alerts and to make recommendations to County stakeholders.

Contractor shall have a single point of contact on the account responsible for Root Cause Analysis (RCA), making sure that all RCAs meet the required deadlines and service level agreements (SLAs). As issues are worked—for those that require an RCA or for which an RCA has been requested—the SDM for each business group shall make sure that they are completed within the SLA timeframe and they are ready for customer review and approval.

Each business group shall have regularly scheduled meetings that the SDM shall be required to attend and report status as needed for all things operational and that fall within the scope of their duties. Because the SDM acts as a point of escalation, they shall assist the client with answers and resolutions by establishing the proper points of contact and making sure the issue is being worked or obtaining and providing the information required.

If an emergency or disaster occurs in a specific business group, the SDM for that unit shall take primary responsibility as needed to support the customer. They shall handle the requests, communications, and so forth required for these events. If the event is something that requires 24x7 support, Contractor shall provide the necessary resources to cover shifts and see that the SDM has adequate support. If an emergency is declared that impacts the entire County and the Office of Emergency Service (OES) activates, the SDM for the Public Safety Group (PSG) shall begin the rotation along with the enterprise service delivery manager to establish required communication and coordination, and the SDMs shall enter that rotation along with Contractor account management to support the effort until Contractor is notified to stand down.

The ESDM shall be responsible for leadership of all SDMs and shall provide continuity across the business groups and the account. The ESDM shall have a direct interface with the County Technology Office (CTO) to make sure that all parties are aware of anything that is going on in the environment and to make process changes/suggestions as needed for continuity of operations. The ESDM shall be embedded with the customer three days per week in the CTO and shall attend all business group meetings as requested. The ESDM shall be responsible for all delivery aspects and SLAs associated with each area for the account on the operational side: service delivery management, Service Desk, End-User, infrastructure services (data center and local), print center, network services, release management, change management, problem management, incident management, and configuration management.

The SDMs shall be responsible for understanding all service frameworks and how they impact their business group as well as for making certain that proper communication and discussions for that framework take place and that resources are available to support all service delivery initiatives. The SDMs shall be familiar with and facilitate adherence to County requirements and information infrastructure.

- Deployment plan for resources and use of facilities

The SDMs are required to have face-to-face interaction with their business groups in addition to email, phone, etc.

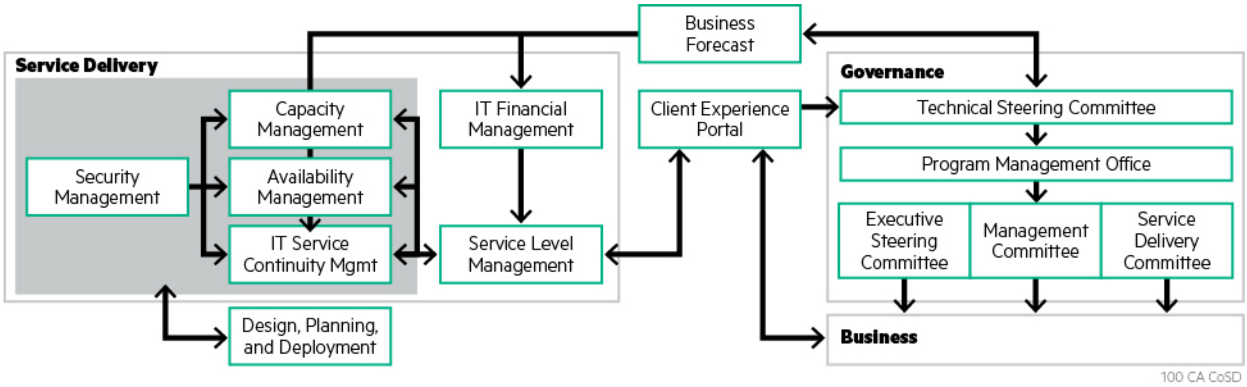
- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's approach to service delivery, illustrated in the figure below, shall enhance the stability and integrity of the services environment through proactive service-level management and governance, transparent service visualization, and analytics that support cost-effective service improvements through integrated availability, capacity, IT service continuity, and financial management. They shall include the following key service delivery disciplines:

- **Availability Management** – The mission of availability management is to understand the availability requirements of the County and to plan, measure, monitor, and continually strive to improve availability of the services and the County's IT infrastructure.

- **Capacity** – Contractor performs capacity planning regularly as well as when new business and application growth are anticipated, when changes to the existing business are anticipated or occur, or when configuration changes are performed within the systems. As part of Contractor’s ongoing capacity review and planning process, Contractor shall coordinate with the County regarding future business plans and computer resource requirements.
- **IT Service Continuity Management** – Contractor’s business continuity professionals shall collaborate with the County to keep its IT Service Continuity Management (ITSCM) plans current, relevant, and executable and to see that they support County operational continuity plans.
- **Service Level Management (SLM)** – The County and Contractor establish a shared view of the services, service-level achievement, and analytics through regular service delivery reviews and IT Service Management (ITSM) Client Portal dashboards. Contractor’s account leadership team shall collaborate with County stakeholders through service delivery reviews and frequent direct dialog to continually review SLAs to make sure that services remain cost-justified and aligned to the County’s business needs. The ITSM Client Portal provides continual “Voice of the Client” feedback to Contractor and relays performance feedback at any time, with top-level visibility to Contractor’s senior leaders.

Contractor’s Service Delivery Model



Service delivery integrates availability, capacity, IT service continuity, IT financial, and SLM to enhance the stability and integrity of the services environment.

The following sections provide additional detail about the service delivery processes depicted in the diagram and summarized in the figure above.

Availability Management

Availability management shall contain the following key activities:

- Assess availability requirements
- Develop and maintain the Availability Plan
- Analyze current availability
- Maintain availability

Capacity Management

Contractor shall perform capacity planning regularly when new business and application growth are anticipated and when changes to the existing business are anticipated or occur, and when configuration changes are implemented in the systems. Capacity management shall meet the following key objectives:

- Verify that optimum IT capacity exists always

- Proactivity
- Reliability
- Outage prevention
- Provide clients with sufficient capacity to support agreed levels of service
- Forecast future requirements for IT resources.

Service Continuity Management

Contractor's business continuity professionals shall work with the client to be sure that ITSCM plans are current, relevant, and executable and that they support the County's business continuity plans. The ITSCM process shall be comprised of the following key elements:

- **Define, Implement, and Maintain the ITSCM Plan –** Contractor collaborates with client business continuity teams to define, implement, and maintain an ITSCM plan that is based on Disaster Recovery Institute International (DRII) and Business Continuity Institute (BCI) standards. The plan is continually updated and assessed through scheduled reviews, as changes are made to the IT environment and as improvement opportunities are identified through testing and execution of the plan.
- **Exercise and Execute the ITSCM Plan –** Contractor's IT service continuity staff shall support the client when conducting required testing and activating plans during a disaster. Contractor shall document and maintain the Contractor staff's IT service continuity procedures to restore the hardware and operating system and the subsystem environment. Contractor operations shall support application recovery testing, such as loading tapes or initializing data storage devices. Joint testing of the IT service continuity plans is conducted through a disaster simulation process based on established test schedules. Contractor closely monitors and document test objectives and actual test activities. Contractor reviews the results of each test and enter any problems encountered in the problem-tracking tool for follow-up and implementation of corrective action. This process enables continual improvement of the recovery plans. Retests shall be performed for tests that do not meet predetermined objectives unless mutual agreement deems retest to be unnecessary.
- **Manage Service Continuity Escalation –** Throughout a service continuity event, Contractor shall manage the agreed escalation procedures to keep the client and Contractor leaders informed, obtain required approvals, and restore service operations in accordance with service levels, thereby minimizing the impact to business operations.
- **Supplemental Assets –** Available for use on the County's program, Contractor has ITSCM-based templates for documenting the following: Business Impact Analysis, Gap Analysis, Continuity Planning Checklist, Threat Analysis, ITSCM Plan, and ITSCM Exercise Workbook.

Service Level Management

Contractor shall work with the client to verify that the levels of service Contractor delivers meet County business objectives.

Security Management

Contractor shall complete a Security Management Plan (SMP) modified from its proven template to identify those security-critical items whose failure could lead to a breach of system security. Contractor shall document a security assurance strategy to minimize or eliminate the potential for system security breaches. Contractor shall review and update the SMP as necessary throughout the program life cycle.

Approach to the role of the Service Delivery Manager (SDM), including SDM operational authorities across Service Frameworks, key functional activities, and metrics to measure the effectiveness of the SDM role.

The SDM shall work closely with counterparts from the County team, outside vendors, and Contractor teams to facilitate a successful initial and ongoing services delivery engagement. This role—essential to managing a small team of technical and business people—shall require varied expertise in the areas of technology, business processes, communications, service provider, and enterprise IT industry knowledge and experience. SDMs shall serve as the face of Contractor services on an ongoing basis for the County in all aspects from supporting pre-design activities and design to delivery, process improvement, and escalation management."

SDM responsibilities and deliverables shall include the following:

- Serves as primary interface for all client contact related to the Contractor services, involved in pre-design and post implementation interface with County and Contractor services leadership teams
- Responsible for County relationship management and total customer experience
- Works closely with senior management and across functional groups to develop effective strategies and programs to meet service delivery goals, including tracking and reporting key milestones
- Responsible for making certain that Contractor complies with agreed services scope and quality
- Provides compliance with established policies, practices, and processes defined by Contractor and County personnel for delivering converged infrastructure related services
- Provides work direction and strategic direction to reporting managers and employees
- Works closely with Contractor lead partners in ensuring a successful services delivery engagement

Metrics to measure SDM effectiveness shall include the following:

- County leadership evaluations—the GITM and ESDM shall meet quarterly at a minimum to discuss how the SDM is providing the services required
- Project performance to goals and objectives
- Meeting scheduled reporting and communication deadlines
- Maintaining agreed certifications
- Annual Performance Reviews by the ESDM
- Customer relationship management skills and meeting objectives
- Identifying opportunities for improvement within their respective business group

2.8. [Reserved]

2.9. Project Management Services

2.9.1. Process and Procedures

- Description of solution to meet the requirements

The Contractor Enterprise Project Management Office (EPMO) is an organizational body that shall be assigned to centrally coordinate the management of in-flight programs and projects across all towers of the Agreement.

Solution: The EPMO shall be responsible for aligning its activities with the County's mission and maintaining an outcome-focused and metric-centric program management organization. To accomplish this, Contractor shall incorporate measured steps to retain situational awareness of the budget, schedule, and risks as well as opportunities for continual improvement throughout the program's life cycle. The EPMO strengthens day-to-day communications and prepares detailed recurring reporting to promote the highest level of transparency and collaboration between the County and Contractor.

Contractor shall use industry-standard practices as set forth by the Project Management Institute (PMI's PMBOK), Software Engineering Institute (SEI's CMMI), and Information Technology Infrastructure Library (ITIL). Contractor has its own Enabling Delivery and Global Excellence (EDGE) process, which is its overall framework for enhancing effective planning, execution, tracking, and reporting of projects. The Contractor team shall use one or more of these best practice standards to create procedures that enable each framework to efficiently perform project management activities appropriate for the nature of its work.

Contractor EPMO guiding policies shall include:

- Identify and use global best practices as a framework for creating tailored, relatable, and customer-centric procedures that provide the best fit to meet Contractor's customers' evolving needs, while driving quality and expedience into Contractor's delivery model.
- Provide frequent, accurate updates to the County Project Sponsor
- Make sure of thorough and timely communication across all framework projects and procedures
- Apply the principle of delivering projects on time and within budget that fulfill the approved requirements
- Promote an environment of continuing education for Project Management Professional (PMP)-certified PMs and for those who aspire to be PMP certified
- Work with Contractor's County partner on continuous improvement processes and initiatives.

These policies are designed to influence and determine decisions and actions when tailoring the processes for the County and ensuring that Contractor's processes conform to PMBOK, CMMI, and ITIL.

The Contractor EPMO person shall chair weekly meetings to make certain that cross-framework coordination, integration, and communication occur for projects and processes. Communication between all frameworks is critical to successful delivery of products and services.

The EPMO shall be committed to coordinating multi-framework projects between the frameworks, and to certifying that there is a lead project manager and project status is reported in a timely and consistent manner. EPMO shall provide a central point for managing processes and standards across all frameworks to enable consistent delivery.

Contractor shall use a formal process change board to identify and implement process improvements that drive quality and expedience throughout the project life cycle. The HPE EPMO shall chair these efforts and support documentation, training, and process reengineering that may be identified through these efforts.

In addition to the standard project management solution described above, Contractor shall consolidate Infrastructure Project Management efforts into its project management service. This provides value to the customer while continuing to facilitate Contractor's goal to integrate all project management services under one set of best practices.

Rationale:

The EPMO shall drive the standards for project management across all portfolios, but shall remain agile where necessary to meet the needs of the specific project/client.

- Deployment plan for resources and use of facilities

The EPMO and project management staff shall be centrally located at the Contractor's Rancho Bernardo facility. Contractor shall join the County at its facilities when necessary to drive successful communication at the program and project levels. This facility approach enables interaction between the project management staff and all customer and Contractor portfolio towers, including:

- County Technology Office (CTO)
- County Group IT Management (GITM)

- County Department IT Coordinators
- County Project Sponsors
- Contractor Account and Operation Management
- Contractor Applications Portfolio Management
- Contractor Infrastructure Operations
- Contractor Account Security
- Contractor Technology Office
- Contractor Business Management
- Contractor Contracts Management

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's proven methodology for effective program management support, EDGE, includes all information needed for Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE shall support all individuals in each ES business unit by providing best practices that they can leverage and use in their daily work.

The EDGE environment shall cover multiple life cycles that can be selected, customized, and integrated as needed for each program. Project and program management shall be integrated through their own life cycles, which conform to PMI PMBOK industry standards, as well as CMMI and ISO. Engineering practices, such as Infrastructure, COTS, and other Enterprise application areas, shall integrate seamlessly with the Project/Program Management areas for project success. EDGE has been customized to the County's needs and processes. EDGE shall be regularly updated to provide End-Users with the most current industry best practices, as well as continually aligning processes and assets with changes in industry standards of PMI, CMMI, ITIL and ISO.

Using the aligned HP/County organizational structure, Contractor shall implement formal communication procedures that engage internal and County stakeholders. Examples of interactions include the following:

- Establishing communication strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communication plans
- Creating EPMO announcements followed up by direct communication with impacted stakeholders
- Developing and maintaining communication vehicles such as the EPMO SharePoint
- Creating and executing communication plans for EPMO initiatives
- Preparing presentation material for internal and external reporting.

Standardization and optimization of Project Management practices across a diverse environment such as the County

The Contractor EPMO and County CTO partner shall be responsible for the integration of these processes across the County enterprise so that service performance can be managed seamlessly. Contractor's EPMO personnel shall facilitate the development of processes, manage the deployment, and provide oversight and management for process execution. Contractor's EPMO personnel shall also establish key roles for ownership and governance of each process, working collaboratively with the County to speed delivery of services focused on quality and adherence to standards.

Internally, the project management team shall meet regularly to escalate issues and to discuss project management measurements and trends. They shall receive training on updates to client processes, industry best practices, and new tools. Contractor additionally shall monitor and meet with subcontractors to make sure they comply with County and project requirements. Contractor shall make certain that subcontractors are aware of and participate in issue and risk management, and that they provide timely accurate status reports.

Contractor shall provide training for project managers, including acceleration programs for the PMP, CAPM, SPI, and other disciplines. Project managers and business analysts shall be encouraged to join and participate in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, the State/Local

Government / Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice, for additional training and shared understanding of best practices across the community.

PMI chapter and PMI/PPM event participation shall also be encouraged across the organization.

Contractor's PPM Academy shall provide regular opportunities for learning.

The EPMO shall share in-house opportunities for PM training sessions or vendor sessions, or PM-specific conferences in San Diego, and inform the County that it may participate.

Contractor shall leverage the best practices of Project Management Plan development and right-size the project for specific County needs. Project Management Plans shall contain one or more of the following sections:

- Scope Statement
- Known Risks and Issues
- Assumptions and Dependencies
- Stakeholder Matrix
- Milestones
- Cost/budget Baselines used in calculating SLs and project success
- All Project Deliverables
- Preliminary Risk Log
- Phased Implementation Approach.

Project schedule templates shall be maintained in the Program and Project Management Center (PPMC). Each framework shall have one or more templates that meet the needs of their particular project tasks.

Contractor shall conduct risk analysis and planning early in the project life cycle with the help of all stakeholders. Monitoring risk and updating the risk matrix shall occur continually during the project life cycle.

For the Applications and Infrastructure frameworks, change management shall follow the formal change request process that flows through CTO and is signed by County and Contractor.

County-facing project status reports shall be made available so that authorized County users and Contractor team members can view the status of a particular work request. Status reports for projects shall be posted on a weekly basis.

All PM work products, status reports, processes, and templates shall be centrally located/managed and shared using DocVault.

Each project manager shall be responsible for establishing and conducting project meetings with his/her customer.

Third-party vendors working with Contractor to implement solutions shall be treated as project team members and held to the same process standards required by the County and Contractor. From the point of project kickoff, the Contractor project manager shall be responsible to direct County vendors on their roles and responsibilities for supporting County projects and required deliverables. These responsibilities shall include following County-approved methodologies and processes and any project status reporting requirements.

In addition to requiring all vendor project participants to follow County-approved project process, Contractor shall also identify potential project risks as part of the upfront project risk assessment and shall include specific mitigation plans for issues that may arise when operating a project that uses third-party vendors. Those risks shall be managed and monitored for risk triggers throughout the project lifecycle.

Measuring and analyzing trend data related to the effectiveness and timeliness of Project Management processes and methodologies.

The Project Management Office shall work directly with County representatives to recommend and identify the critical performance indices that provide useful project trends and status. Project trends shall be calculated and reported on a regular basis by the Project Management Office and discussed as part of weekly project review meetings. Trends related to project schedule, budget, and other key performance indicators shall be monitored on active projects in Contractor's Project and Program Management system. If Contractor identifies unfavorable trends, it shall perform a root-cause analysis to isolate new causes of trends, and provide coaching assistance to project managers to understand the root-cause and provide corrective and preventive action.

The County has designated two critical SLAs around the KPIs of Schedule Performance Index (SPI) and Cost Performance Index (CPI) on Discretionary Standard projects. Contractor shall support these KPIs throughout the project lifecycle, measuring progress and reporting on earned value. Contractor shall constantly manage to these metrics throughout the project lifecycle.

Contractor shall implement the following or as otherwise stated in the Standards and Procedures Manual:

- KPIs for Project Estimate Accuracy and Response
- KPIs for Impact, Priority, and Mitigation of Risks/Issues
- KPIs for Project Change Management
- KPIs for Projects Opened, Closed, Delivery Times, etc.
- KPIs for Defect Management
- KPIs for Project Schedule Management/Milestone Comparisons

Contractor shall continue to identify additional KPIs best suited for the project management organization. The County and the Contractor PMO shall meet regularly to discuss overall objectives, issues, and improvement items, which can be incorporated into ongoing KPI development and improvements.

The Project Management Office shall use tools to collect and measure the effectiveness of estimates against actuals for all standard projects from initiation to closure. Contractor shall review trend reports regularly, along with individual reporting per project. The data collected shall include estimates at initiation, actuals by role at closure, total project CPI/SPI, number and type of change requests, and cost impacts. Contractor shall also collect data to determine the effectiveness of ROM estimates for project management and engineering project activities and continuously update the Basis of Estimate process and provide more accurate and predictable ROM estimates.

Relationship between project managers and Service Framework resources

Where possible, the same project resources engaged for creating project ROM estimates shall also be responsible for delivering the end product. This approach drives a high level of accountability and quality for Contractor's solutions.

Starting with the project's initial estimate, Contractor shall engage the solution frameworks to provide rough estimates for the project's proposal. Once a project is approved by the County, Contractor shall initiate an internal kickoff with the team, and the project manager shall engage the framework leads to determine the level of resources and effort needed from the initial requirements gathering through deployment. Requirements Development and Planning shall engage the framework resources to refine the solution and further refine the estimate of resources needed to deliver. During execution, testing, and deployment, the various frameworks shall be actively engaged in providing and testing the solution, and positioning for, executing, and supporting deployment. At project closure, the framework resources shall continue their involvement to make certain that warranty-period support is available, turnover to production is successful, and project close-down ends with a final collection of effort and lessons learned. These touchpoints shall be embedded in the standard project plan templates and reflected in the project management life cycle.

Throughout this processes, Contractor shall identify framework SMEs from operational support when needed to advise and provide critical product information and input to the project team while supporting the operational needs of the product.

Use of Tools

Project and Portfolio Management Center (PPMC) shall be Contractor’s Primary Project and Portfolio Management (PPM) tool suite. Contractor shall use PPMC for the development and ongoing management of project schedules, small project work, LOE-based work, operational support work, budget tracking, and status reporting. Contractor shall also use it to track program-level, high-visibility initiatives with multiple projects, and at the portfolio level to manage and track projects with competing resource needs within a business group.

- Contractor shall use SharePoint as a storage repository for project artifacts, enabling easy access of project standards, methodologies, processes, and procedures; storage and access of project templates; and storage and access of project-specific documentation such as specifications, project plans, etc.
- Basis of Estimate: Contractor has developed a unique Rough Order of Magnitude (ROM) tool that the EPMO shall use to support expedited and thorough estimates that the County needs to secure funding for its initiatives. This tool is based on PMBOK-defined procedures for estimating while accounting for County-specific processes when developing an estimate. It enables the project manager to define the project work in terms of complexity/risk and a standard list of deliverables and tasks which follow the development methodology selected and client requirements at the early stages of a project. It provides ranges of estimates based on the input and historical estimates and actual effort from past projects. This customized tool takes into account client and Contractor processes and life cycles, and documents decisions and assumptions made for planning. This tool is managed internally, and automates the creation of client-facing deliverables, including the Budgetary Estimate Cover (an authorizing document). The EPMO team tracks performance of estimates to actuals on projects and uses that data to further inform and improve the BOE tool and improve the quality of Contractor’s estimates to the County client.

The following table shows additional Contractor automated tools and methodologies.

Contractor Automated Tools and Methodologies

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION	
Service Portal	Acts as the single, virtual, and centralized source of information for all County stakeholders and HP. The Portal shall provide access to the following:	
	• Consolidated program reporting • Service levels reporting	Contractual information Contractual deliverables and plans
Project and Portfolio Management Center (PPMC)	• Consolidated project management tool • Budget management and labor billing source • Schedule management • Resource management • Risks and issues management • Project status reporting	

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION
County Document Repository (DocVault)	Workspace and final repository for all project-related deliverables and account-wide policies and procedures
Program and Project Management Methodology	Includes templates that outline scope, risk, quality process, personnel, cost, schedule, communication, and procurement management responsibilities
Service Delivery Dashboard and Voice of the Client (VoC)	Provides clients with program performance and enables them to provide direct feedback to Contractor executive leadership

For internal tools such as the above that are used to the support the County's business, Contractor shall conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that Contractor is using the right technology to support the County's needs and remain in supported status.

2.10. Integration and Testing Services

2.10.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall use a comprehensive testing framework that includes the structure, processes, tools, and templates to enable consistent, high-quality testing services and deliverables. Contractor's testing framework shall verify compliance with the application development process and shall validate the quality of the application to address the commitments outlined in the SOW. Contractor shall achieve maximum integration testing efficiency by grouping testers separately from developers.

Contractor shall first work with the County to determine the level of strategy that best meets its needs. Contractor shall review the current strategies, testing requirements, business needs, and priorities to develop the most efficient and cost-effective testing strategy for the SOW project.

Contractor shall supplement and support the project life cycle with the following testing-specific information:

- Testing roles and responsibilities
- Testing methodology
- Test levels to be performed
- Test coverage to be performed for each test level
- Test deliverables
- Test management and measurement approach
- Required testing environments and tools.

Based on the priorities identified in the test strategy, Contractor shall develop a Test Plan that covers each required test level and provides tactical guidance by specifying the following factors:

- **Test Scope** – Scope of Contractor's testing services to be provided, including test types
- **Test Schedule** – Schedule for all phases of testing, integrated with the overall project schedule (test development, test execution, testing metrics collection, and testing reporting)
- **Test Roles and Responsibilities** – Test roles/responsibilities for all participants, including the Contractor team, County staff, and third-party vendor staff; responsibility for test environments and tools
- **Test Design/Methodology** – Test case design techniques/strategy for each test level

- **Test Procedure/Execution** – Test-level execution tasks, including participants, to conduct execution; entry, exit, pass/fail, suspension, and resumption criteria for each test level
- **Test Tracking and Reporting** – Test results data collection requirements, documentation, and reporting; test progression tracking and error/deficiency management/resolution process; risks specific to a test level that require mitigation.

The Contractor Test Plan shall also outline the recommended testing tools and testing management and measurement.

Contractor shall apply and adapt the processes, techniques, and templates of its testing method to effectively manage and control the planning, execution, and completion of all testing activities. Testing management and measurement shall involve the following actions:

- Establishing and maintaining detailed estimates, a test schedule, resource plans, and procedures for all testing phases
- Managing preparation of test plans, scenarios, and test cases for each test level
- Establishing acceptance criteria
- Managing the execution of test cases, tracking and resolving defects, and verifying completion of tests, including regression testing
- Managing testing close-down, including reporting.

To make sure the application is ready to move into production, Contractor shall apply comprehensive metrics, supported by standard testing management tools. Contractor shall generate reports to provide insight into the status of testing throughout the project. With this information, Contractor shall confirm that tests are mitigating risks on high-priority requirements. These metrics shall support timely corrective action and informed decision-making by all project stakeholders, particularly “go/no-go” decisions to progress through project phases.

System testing shall involve testing both an application and its supporting infrastructure. Contractor shall provide system testing to establish confidence in End-User acceptance of the system and that the system is functionally and structurally stable, reliable, secure, and interoperable. System testing shall encompass an integrated system or a logical subset of application functions. It shall verify compliance with functional and nonfunctional system requirements and specifications. The process normally involves creating test conditions for evaluating the application and its infrastructure.

Contractor shall prepare and perform system tests based on approved requirements documents, the application architecture, and the application design specified by the development team. Contractor shall create tests to exercise the specific business functions selected and submit them for County approval. This approach helps to validate that the system performs according to the County's requirements.

System testing shall include testing interfaces with external entities and with batch and online software. All parts of the system shall be available for system testing to succeed. Data shall enter through normal interfaces so Contractor can test interaction between various subsystems. If the County does not have an appropriate testing environment available to accept transactions or files, Contractor may use emulators to simulate interactions with external systems. System test activities shall include the following:

- Test cases, standard and ad hoc
- Test data management
- Requirements Traceability Matrix (RTM)
- Performance benchmarks when applicable
- Summary report.

Contractor shall use automated life cycle management (ALM) tools and techniques as it develops system test cases based on functions and roles. Function-based tests validate the application's functional requirements and data flows. Role-based tests shall verify access to the application, menus, submenus, buttons, and icons; verify a complete and correct process flow for each defined role; and validate that access covers only specified areas.

The following table describes Contractor's high-level input criteria, activities, and deliverables for test cases.

Contractor Test Criteria and Deliverables

INPUT CRITERIA	• Baselined test scope, strategy, and plan • Baselined effort estimation and schedule • Baselined defect, change, configuration, communication plan, and risk management plan • Baselined and updated Test Traceability Matrix (TTM) Baselined design, business requirements/specifications, and use cases documents
ACTIVITIES	• Identify functional and technical test scenarios • Update affected test case and script • Design new test cases and scripts: review, sign off, and baseline • Define success criteria and expected outcomes • Design test data: review, sign off, and baseline • Collect metrics Update test traceability, arrive at test coverage, and sign off
DELIVERABLES	• Baselined test cases, scripts, and test data • Baselined smoke test suite • Baselined test traceability Sign-off by stakeholder

Contractor shall implement the database approach to test data management.

The RTM shall trace downstream work products of the requirements, such as design, code, and test cases. If an RTM exists, the Contractor testing team shall update it when the initial test design is complete, to map requirements to test cases. If an RTM was not developed, Contractor shall establish one while developing test cases, linking each test case back to the original requirement.

As Contractor executes test cases, it shall document and map any defects it encounters to the corresponding requirements in the matrix. The updated matrix shall provide a running record of how testing has addressed and met each requirement, revealing gaps the testing team needs to fill and opportunities to consolidate redundant tests.

The County shall receive a complete overview of system testing results in a system test summary report, which shall include an overview of the approach, tools, test cases, activities, results, and any outstanding defects.

System integration testing shall confirm that the necessary communications and setup exist to perform functional testing and shall address the need to assess whether the system interfaces smoothly with other applications or systems.

After the development team provides the testing team with the interface code, Contractor shall perform system integration testing. This testing is often the most complex because it normally involves communication and security layers and requires coordination with outside organizations.

Certain applications may involve providers external to the individual SOW. When testing with an external organization, Contractor shall provide that group a copy of all test cases to review to support test coordination and data synchronization. To support external interface testing, Contractor shall work closely with the County project manager to coordinate and cooperate with third-party interface owners.

In conducting performance testing, Contractor shall 1) understand the performance requirements; 2) determine the types of performance tests and the test volumes that best meet those requirements; 3) test the system performance; and 4) ensure the new change does not impact existing functions or systems. Contractor shall also assist the County with performance tuning recommendations to help fix performance-related issues. Contractor's methodology shall include the following actions:

- Identify and scope requirements
  - Performance test requirement analysis, review of volume metrics and performance goals
  - Performance test strategy and planning
  - Arrive at scope effort, cost, and timeline
- Determine performance testing type
  - Load testing
  - Stress testing
  - Volume testing
  - Scalability
  - Failover testing
  - Regression testing
- Review and provide recommendations of performance test scenarios and volume metrics performance goals provided by the project team
- Develop performance test strategy, test plan, and scripting standards
- Set up and maintain the test environment, including build and deployment activities
- Prepare test data for project owner's review before baseline
- Design, execute, and analyze performance test for approximately four performance test scenarios identified and provided by the project team
- Provide required support for the performance tuning team, such as re-execution of scripts to identify replicating issues.

The following table presents detailed performance and load-test strategy.

Contractor Performance Testing

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
Discovery Phase (Requirements Analysis and Performance Test Planning)	• Application non-functional requirement specifications (SRS, design specifications, and so forth) • Business scenarios, performance test scenarios, use cases • Performance goals and volume metrics • Release scope • Production environment details	• Conduct requirements study • Determine test scenarios and impact analysis • Identify test scenarios for performance testing • Develop performance test strategy/plan • Derive test environment specifications • Conduct performance test scenarios, test strategy/ plan, traceability, review, and approval	• Performance test strategy/plan • Identified test scenarios for performance testing

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
Performance Test Environment Preparation/ Readiness	• Performance test strategy, plan • Tools and licenses • Application builds • Performance test environment • Functional test cases • Performance test scenarios, test cases and test data, sample test data • SRS, design, other specifications	• Set up and configure test environment • Deploy and configure application build • Identify performance testing tools, monitors, installation, and setup/configuration • Test data preparation, review, and baseline • Test environment and build validation through sanity testing	• Performance test environment with latest build • Performance test data • Performance test tools installed and configured
Performance Test Design/ Development	• Performance test scenarios • Identified performance business scenarios • Performance test plan • Test environment with latest stable build • Performance test data • Performance test tools installed and configured • Baselined performance business and test scenarios	• Develop performance test scripting standard • Develop performance test framework • Develop test scripts/test suite (integration of test scripts) • Develop test data files • Identify and review performance test metrics • Review and baseline all above test artifacts	• Performance test framework/ harness • Baseline performance test scripts and test suite(s) and associated test data and configuration files
Performance Test Execution, Analysis, and Reporting	• Performance test strategy and test plan • Test environment with latest stable build deployed • Baseline test scripts • Non-functional requirements (performance goals and volume metrics) • Test environment sanity test and all test entry criteria	• Validate test entry criteria • Execute performance test • Validate test exit criteria • Analyze and report performance test results • Collect performance test metrics • Log and track defects	• Performance test execution status reports • Performance test results, performance issues, bottlenecks, metrics reports • Sign-off report
Performance Tuning Support and Post-Tuning Testing	• Performance test results and reports • Performance test results analysis report and recommendations for tuning • Performance goals and volume metrics • Test entry/exit criteria	• Validate test entry/exit criteria • Provide performance-tuning support • Provide post-tuning retesting of scripts • Conduct result analysis of post-tuning tests • Provide performance test reporting for post-tuning tests	• Post-tuning test results • Post-tuning performance test reports • Final sign-off on performance test report

To identify and correct vulnerabilities before the application goes into production, Contractor shall provide Security Testing Services, which shall make sure the County's applications are protected against exposure to hackers or other threats to their integrity, availability, or confidentiality. Security Testing Services shall help the County achieve the following goals:

- Improve coding and security practices
- Identify and eliminate or mitigate security vulnerabilities in web applications
- Comply with regulatory and reporting requirements
- Test existing applications and quickly address major vulnerabilities
- Cut overall project costs by identifying problems early.

To address security risk levels associated with unique applications, Contractor shall provide vulnerability code scanning and application security testing. Contractor shall work with the County to assess the application risk level, then recommend the types of security testing required.

Contractor shall provide vulnerability code scanning for medium-security-risk applications. First, Contractor shall scan the code to identify critical vulnerabilities, then Contractor shall assist the development team with remediating issues and applying regression testing code fixes to address these vulnerabilities.

Contractor shall provide application security testing in the testing environment for high-risk web applications to uncover security vulnerabilities before moving the application into the production environment. Contractor shall assist the development team with remediation and regression testing of code fixes to address the vulnerabilities uncovered.

Regression testing shall involve selectively retesting previously tested functions and running selected test cases to make sure that new development and defect fixes have not introduced or revealed new faults. Regression testing can occur throughout testing and shall be executed whenever the build changes. It shall occur at all test levels of Contractor's Enterprise Testing Methodology and throughout development.

During test case development, Contractor shall identify candidates for regression testing. Contractor shall then use these cases to test future application releases. The following changes shall typically require regression testing:

- Addition of new business functionality (new modules or sub modules, new business transactions, new business processes)
- Modifications to current functionality (enhancements, defect fixes) for a release
- Implementation of the current application to new locations
- Upgrades to more recent versions of the application or operating system
- Hardware upgrades.

Business regression testing shall focus on the critical, high-volume business processes for all business functions introduced, up to or including the previous software release. Contractor shall build on previous regression tests by adding new scripts with tests based on the last release's functions. Contractor shall focus specifically on known high-risk areas.

Contractor shall provide the option to perform regression testing after completing a major type of testing (such as system testing) but before releasing the application to the next test level.

- Deployment plan for resources and use of facilities

Contractor's key facilities shall be in Rancho Bernardo, CA; El Paso, TX; Pontiac, MI, depending on skillset required.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's testing methodology shall align with the industry-accepted Testing V-Model.

Contractor's risk-based, requirements-driven testing approach includes the following components:

- **Ambiguity Analysis** – While performing requirements validation, Contractor shall systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize inconsistencies and maximize clarity. This process helps to meet users' expectations; gives the project team a targeted and complete plan; and builds common understanding of requirements for project managers, developers, testers, and users.

- **Risk Analysis** – Risk-based testing shall focus on analyzing risks to reduce misdirected or incomplete test coverage. Contractor shall systematically analyze requirements to determine the priorities that guide the testing strategy. All stakeholders, including third-party interface owners, are engaged in these analyses. Contractor shall define test environment requirements early in the life cycle.
- **Systematic Test Design** – Through methodical activities focused on managing and mitigating risks, Contractor shall apply test design techniques to plan, choose, and develop the most effective tests to deliver the required amount of testing.
- **Requirements Traceability** – Throughout test development and execution, Contractor shall update the RTM to comprehensively depict test coverage and to keep testing focused on high-risk, high-priority requirements. Because each test case inherits priority from its requirement, the RTM helps the team analyze the testing impact of any requirements changes.
- **Testing Metrics Collection/Reporting** – Contractor shall use testing reports to gain ongoing insight into the progress of tests and defect resolution, and Contractor shall offer timely opportunities for mitigation of a risk before it causes harm to the County's environment – or to the application itself.
- **Testing Close-Down Activities** –Contractor shall focus on satisfying high-risk, high-priority functionality first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements as agreed to by the County. As part of project close-down, Contractor shall either transition the work to the County, as outlined in the SOW, or continue providing maintenance and support.

2.11. Incident Management Services

2.11.1. Process and Procedures

- Description of solution to meet the requirements

As a part of this process, all incidents shall receive prioritized attention, depending on severity, Service Level Agreement (SLA), or the immediate service restoration needs of the County.

Solution: Contractor shall use an IM process that includes ITIL methodology.

Contractor's focus shall be:

- Restoration of service operations as quickly as possible using repeatable streamlined processes and escalation points
- Frequent, clear, and concise communications to End-Users and CTO through resolution
- Minimizing the adverse impact of incidents on the business
- Providing departments and End-Users with a single point of contact (POC) for all incidents reported
- Maintaining portal-based visibility into incidents and trouble tickets with drill down to detailed information.

Contractor shall provide full life cycle IM through its Service Desk and IM functions. The Contractor Service Desk shall act as the initial POC for the identification, categorization, and tracking of all County incidents in its service management system. This system shall provide the efficient assignment of incidents for resolution by the responsible teams and direct access to incident status by County personnel. The system shall also objectively measure accountability for all aspects of the IM process.

- Deployment plan for resources and use of facilities

Incident management shall be supported by the following groups:

- Service Desk
- Service Delivery Managers
- Applications SMEs
- Datacenter SMEs (network, storage, exchange, BUR)
- Local account server team/Infrastructure SMEs
- Desktop and Remote Support Technicians, as needed
- AT&T
- Engineering and Architecture

The majority of the services provided by this process shall be supported by the account team at Contractor's Rancho Bernardo site; AT&T shall provide services from Trade Street site.

Supplemental support for datacenter and other areas supported by leveraged frameworks shall be provided by the account team in Rancho Bernardo. The Service Desk shall provide support from Pontiac, MI.

- Key methodologies and processes in solution including year-to-year continuous improvement

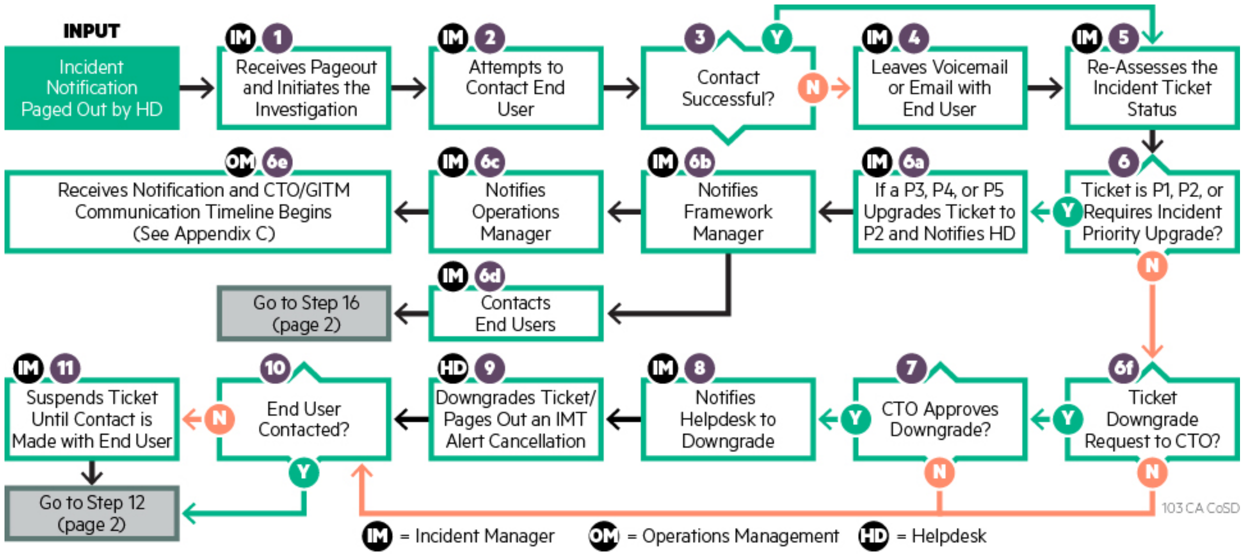
The Service Desk shall serve as the primary point of contact and owner for the identification, categorization, monitoring, and tracking of all County incidents within Contractor's service management system, providing efficient assignment of incidents for resolution by responsible resolver teams and direct access to incident status by County personnel. The system shall also objectively measure accountability for all aspects of the IM process.

The Contractor SDM team shall continually monitor incidents, responses, escalations, and resolution activities through the ticketing system for compliance with procedures and performance objectives. The Contractor SDM shall provide key configuration items (CI) for incident components. During major (high severity/scope) incidents, the SDM team shall actively facilitate status notifications and escalations to all appropriate levels in customer and vendor organizations. Contractor shall provide the right people, processes, and tools to perform comprehensive IM for the County, who shall receive timely responses to questions and issues as they occur and progress through the incident life cycle.

The Service Desk and SDM team shall refine a mature process for full life cycle IM. Each sub-process and step is described in the figure below. This process shall assign Level 1 support responsibility to the Contractor Service Desk, which shall also be responsible for incident recording, categorization, and assignment. The Enterprise SDM shall act as an escalation point and operations orchestrator, helping the County achieve continued high levels of service and End-User satisfaction.

The Contractor enterprise SDM shall be responsible for verifying prioritization and categorization standards for IM processes in collaboration with the County, validating that Contractor records these standards in the policies and procedures and continuously monitor other service providers' compliance with these standards. The Contractor team shall also be responsible for verifying procedures and mechanisms for handling, expediting, and communications of high-priority incidents. These procedures and mechanisms shall be recorded in the Standards and Procedures Manual and also be continually monitored for compliance.

Incident Management Flowchart


INPUT
Incident Notification Paged Out by HD
IM 1 Receives Pageout and Initiates the Investigation
IM 2 Attempts to Contact End User
3 Contact Successful?
Y
N
IM 4 Leaves Voicemail or Email with End User
IM 5 Re-Assesses the Incident Ticket Status
6 Ticket is P1, P2, or Requires Incident Priority Upgrade?
Y
IM 6a If a P3, P4, or P5 Upgrades Ticket to P2 and Notifies HD
IM 6b Notifies Framework Manager
IM 6c Notifies Operations Manager
OM 6e Receives Notification and CTO/GITM Communication Timeline Begins (See Appendix C)
IM 6d Contacts End Users
Go to Step 16 (page 2)
N
6f Ticket Downgrade Request to CTO?
Y
N
7 CTO Approves Downgrade?
Y
N
IM 8 Notifies Helpdesk to Downgrade
HD 9 Downgrades Ticket/ Pages Out an IMT Alert Cancellation
10 End User Contacted?
N
Y
IM 11 Suspends Ticket Until Contact is Made with End User
Go to Step 12 (page 2)
103 CA CoSD
IM = Incident Manager
OM = Operations Management
HD = Helpdesk

The Contractor SDMs shall continually monitor and review incidents within the ticketing system for completeness, accuracy, proper categorization, and timeliness of resolution activities as established by the County and Contractor and defined within the policies and procedures within their respective business groups. Each SDM shall provide operational data and information related to outages and issues, among others, for their respective Business Group. The SDM shall, on a weekly basis, provide reporting of this review to the County Technology Office, operational POCs during the existing weekly Operations status meeting.

Contractor shall continue to document and provide procedures for enhancements related to incident resolution. Scripts, techniques, and step-by-step actions shall be recorded in the knowledge management system, subject to change management processes, for future use by support personnel and End-User access for self-help.

Contractor's IM process shall assign initial responsibility for the identification of problems to the resolving service providers in the problem management process description. If an incident is the result of a change, Contractor shall record the information and refer it to the change management process. If Contractor determines an incident qualifies as a problem, Contractor shall record it in the incident record for referral to the problem management process. Contractor's SDMs shall be responsible for IM and problem management for the business group, and shall verify evaluations performed in this step and escalate incidents to the change and/or problem management process as required.

SDMs shall be responsible for monitoring and managing the entire life cycle of incidents to comply with resolution, status, and notification processes as well as procedure requirements of the Service Desk. As part of Contractor's performance-based management approach to quality assurance, Contractor shall actively monitor and remediate underperforming KPIs and incorporate them into Contractor's continuous improvement process. Contractor shall prepare a quarterly action plan to address service improvement objectives and activities for County review and implementation approval.

Staff and respond to Priority 1 Incidents.

As documented in the County Standards and Procedures, when a Priority 1 incident is received, Contractor shall log it into Service Manager and an electronic alert shall be sent out along with an eNote page to the appropriate support staff. The SDM on point shall receive the page with the incident ticket number and immediately ensure the frameworks are engaged and have begun work on the issue and preps for customer notification. If services cannot be restored within 30 minutes, a bridge line shall be stood up with all frameworks on the call until resolution of the issue. The SDM shall send the first status to the County End-User and CTO within 60 minutes and the status shall continue every hour until service is restored.

The SDM shall monitor and track the incident ticket to closure and provide all required status communications during the incident life cycle. When a change in the status of the request occurs, the SDM shall determine if the ticket issues have been resolved or if the status change is valid. If issues have not been resolved, the SDM shall continue to monitor and track the request until resolution.

If the ticket issues have been resolved, the SDM shall send out final communication and status and proceeds with next steps based on ticket priority. If the ticket is Priority 1 or 2, the SDM shall make sure that an RCA has been created. When the problem ticket has been completed for Priority 1 or 2 issues or a permanent solution has been implemented for non-Priority 1 or 2 issues, the SDM shall document all the actions taken in the activity fields of the ticket and changes the ticket status to Resolved.

Trend analysis of Incidents to identify and correct recurring Incidents.

The Contractor enterprise problem manager shall be responsible for analyzing quality and reporting trends related to incidents. This analysis shall provide recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action shall be taken to correct, improve the outcome, or prevent future outages from occurring. These reports shall be provided on a periodic basis. Contractor's proactive method shall include performance-based management and periodic assessments of Contractor KPIs within the IM framework and shall include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the EPMO status dashboard. Contractor shall also use this data to identify and substantiate trends relating to similar incidents or contributing to problem recurrence, and developing solutions to address chronic issues. Contractor shall continually assess these indicators to identify negative trends. Contractor shall continue to conduct RCAs where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

RCAs

Contractor shall implement the following:

- Once Priority 1 and Priority 2 incidents are resolved, the RCA manager shall enter information into an RCA Submittal Form and submit it to the appropriate SME and framework manager.
- Once received, the Contractor technical SME shall:
  - Gather additional data from other framework SMEs as needed
  - Determine the chronology of events and causes
  - Determine any underlying root and contributing causes and how they manifest
  - Complete the RCA and develop corrective action items/recommendations
  - Complete the RCA Submittal Form and submit findings for Peer and Tower Management Review
  - , submits the findings to the RCA manager once the SME findings have passed Peer and Tower Management Review
- After receiving the findings, the RCA manager shall schedule a formal review by the Contractor RCA team.
- The Contractor team shall then determine if the RCA is complete and, if so, shall address all concerns. The RCA manager shall conduct a final Quality Review and submit it to the RCA team for their final review. On final approval, the RCA shall be submitted to the CTO RCA representative for final disposition.
- This process shall be completed within 6 business days of the final resolution of an incident ticket or receipt of an ad hoc RCA request from the CTO.

- For RCAs related to an outage that is business group specific, the SDM shall make sure all required information is gathered and provided.

Corrective action items that are not completed as a part of the incident resolution in the RCA shall be documented in the Problem Management SharePoint site with an owner and date of completion assigned. This system shall have automatic email alerting assigned to it for the POC to make sure items are completed as required. The Enterprise Problem Manager shall be responsible for validating and verifying that all items are completed on the site within the timeframe that is documented. The HPSM (HPE Service Manager) system shall provide a problem case number for all corrective action items and problems being worked that do or do not have a RCA as a requirement. These Problem cases shall make sure that Contractor has complete tracking and a connection between the incident and the change records required to act on the items that need to be addressed. These cases shall not be closed until all activities are completed and documented.

Detailed processes shall be documented in the Standards and Procedures Manual.

2.12. Problem Management Services

2.12.1. Process and Procedures

- Description of solution to meet the requirements

Problem management shall require the investigation of root causes to memorialize occurrences in the Contractor knowledge repository and eliminate future occurrences wherever possible. The process shall also make sure that corrective actions and resolutions are implemented through the appropriate control procedures, such as change and release management. Active incidents and problems shall be documented at every step and the status shall be accessible for End-User review through the Service Portal.

As Contractor has in place today, problem management systems shall also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time. Although incident management (IM) and problem management are separate processes, they are closely related and typically uses many of the same tools and data points.

Solution: Contractor is assigning a single service delivery manager (SDM) per business group to act as a single point of escalation and communication. Moving forward, Contractor shall take steps that further enhance the ITIL framework, putting more formalization around this process in an effort to continue improvement and to maintain environmental stability.

Problem management shall be under the purview and responsibility of SDMs who shall make sure that all problems are resolved, including root cause determination when necessary. Contractor shall additionally make certain that all problem-related activities be reported and recorded, archived, and made available to County stakeholders.

Rationale:

Problem management shall be a daily responsibility for the SDMs and shall be assigned activities to work—whether it be proactively or through tickets, escalations, or other similar activities. Contractor has an enterprise problem manager who shall report, track, and communicate all problem management issues worked by the team and the account via the weekly CTO operations status meeting.

- Deployment plan for resources and use of facilities

The majority of the services provided by this process are supported by the account team at Contractor's Rancho Bernardo site.

Data center and other areas supported by leveraged frameworks shall provide supplemental support.

The Service Desk provides support from the Pontiac, MI facility.

AT&T provides services from Trade Street site.

- Processes in solution including year-to-year continuous improvement

For Contractor, a problem is any event that has the potential to inhibit the County's ability to perform a business function. Contractor shall provide well-defined processes, key performance indicators, and mature IT tools to alert Contractor's integrated delivery teams when conditions indicate the potential for a problem to occur. Contractor's main goal is to minimize or prevent service degradation to the County's end so the County can continue to perform its duties and service the public unimpeded. Contractor shall train all program team members of these processes, best practices, and lessons learned are shared to maximize effectiveness, promote reuse of knowledge, and optimize project timelines.

Problem Management Techniques and Controls

As a standard practice, Contractor shall conduct enterprise-level delivery reviews weekly to share experiences across the IT services and cross-functional frameworks to identify and mitigate risks.

Recognizing Problems - Contractor uses a methodology-based approach to recognize, address, and correct problems that may arise throughout the IT organization. Contractor's approach combines proven problem management methods and processes, such as root cause analysis, with open communications, transparency, and continuous/iterative feedback. Contractor shall proactively analyze, measure (through leading indicator KPIs), and monitor performance through these multiple channels to increase the probability of identifying and mitigating risks and issues early, before they manifest as incidents or problems.

Correcting Problems – The appropriate SDM shall oversee corrective investigations and problem remediation by designated support representatives. Contractor shall use incident or trouble ticket input as well as procedure manuals, knowledge databases, and other tools to resolve the problem. The SDM shall determine if a workaround can be provided or identify a permanent solution to the problem. Once a workaround or permanent solution is determined, the SDM shall decide on the change needed to implement the workaround or solution. If a Request for Change (RFC) is required, the SDM shall create an RFC. If an RFC is not needed, or after the RFC has been approved, the SDM shall determine whether the implementation of the workaround or solution requires infrastructure support. If needed, the SDM shall create an Infrastructure RFC in Service Desk and link it to the incident.

Resolving Problems among Team Members. If an identified problem threatens the program quality or cost, Contractor shall address the subcontractor directly responsible for the area of nonperformance. In situations where overall contract performance is at risk, Contractor shall issue the subcontractor a written notice specifying the areas of nonperformance.

Subcontractors and the Contractor management team shall meet regularly to discuss overall contract performance. These meetings serve as important forums to identify and resolve potential problems. Open and extensive communication among team members fosters a cooperative atmosphere in which Contractor can jointly resolve problems at an early stage.

Proactive Communications. Contractor's SDM shall maintain transparency with the County through regular communication, reporting on problem progress, and facilitating meetings. The SDM shall be accountable for maintaining the relationships, monitoring subcontractor performance, identifying training needs, and escalating issues that require higher levels of attention.

Staff, address, and remediate systemic and/or recurring problems.

Contractor shall assign an SDM—and an enterprise problem manager—to be responsible for addressing and remediating systemic/chronic or recurring problems. If necessary, this shall be preceded by an in-depth analysis of an issue such as trends associated with tracking Service Desk tickets. Actions can include the use of Cascade to isolate an issue, or creation of a pan-framework tiger team to address chronic or recurring problems.

Trend analytics to identify and correct recurring problems.

The Contractor enterprise problem manager shall be responsible for analyzing quality and reporting trends. This analysis provides recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action shall be taken to correct, improve the outcome, or prevent future problems from occurring. Contractor proactive method includes performance-based management and periodic assessments of Contractor's KPIs within the problem management framework. Contractor efforts shall include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the Enterprise Project Management Office (EPMO) status dashboard. Contractor shall use this data to identify and substantiate trends relating to similar problems or contributing to problem recurrence, and develop solutions to address chronic issues. An integral component of Contractor's continuous improvement process, Contractor continually assesses these indicators to identify negative trends. Contractor shall continue to conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

Root cause analyses (RCAs) to remediate identified Incidents and Problems.

Contractor shall use problem-oriented RCAs to determine underlying causes, identify appropriate resolutions, document findings, and provide recommendations to prevent recurrence of the problems.

5 Whys and the Fishbone Process

The 5 Whys can be used individually or as a part of the fishbone (also known as the cause and effect or Ishikawa) diagram. The fishbone diagram helps Contractor explore all potential or real causes that result in a single defect or failure. Once all inputs are established on the fishbone, Contractor can use the 5 Whys technique to drill down to the root causes.

Steps to Complete the 5 Whys

- Write down the specific problem. Writing the issue helps you formalize the problem and describe it completely. It also helps a team focus on the same problem.
- Ask why the problem happens and write the answer down below the problem.
- If the answer you just provided doesn't identify the root cause of the problem that you wrote down in Step 1, ask why again and write that answer down.
- Loop back to Step 3 until the team is in agreement that the problem's root cause is identified. Again, this may take fewer or more times than five Whys.

2.13. Change Management Services

2.13.1. Process and Procedures

- Solution to meet the requirements and the rationale

The change management process itself is the sequence of steps or activities required to implement County-approved changes into the environment and verify the outcomes are as intended. ITIL methodology is the foundation that Contractor shall provide for change management. Overall, Contractor is an advocate and champion of successful change management as an integral component of Contractor's cross-functional management processes and best practices.

Solution: The foundation of Contractor's change management approach shall be its ITIL certified processes, of which change management is an integral component. A key element of the approach shall be assigning a single service delivery manager (SDM) per business group to act as a point person and to monitor changes that may impact that space. SDMs shall be responsible for making sure that proper communication and discussions for that framework take place and that resources are available to support the RFC owner for testing/validation.

- Deployment plan for resources and use of facilities

Operating out of its Rancho Bernardo facility, the Contractor Change Manager shall implement and sustain repeatable, methodically driven change management processes and best practices. Timely, accurate, available stakeholder documentation is an integral part of the change manager's activities, which Contractor shall coordinate with County counterparts.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor IT Change Management Suite and Services shall support multiple types of change requests and mitigate the risks associated with potential requests. The Change Management Suite shall integrate change processes into the broader ecosystem in a cost-effective way, providing full and open transparency and progress reporting. Contractor's Change Management Suite tool shall assist in the continuous improvement needed in this framework, shall greatly enhance configuration visibility and stability, as well as monitoring the type and frequency of upgrades that may be required.

Contractor IT Change Management shall be part of an integrated set of ITSM process modules for Service Manager.

The Contractor IT Change Management Suite shall come with embedded, out-of-the-box IT Infrastructure Library (ITIL)-based best practices. It shall create mechanisms for measuring change process workflows, automate impact analysis, and enhance Change Request Control Board (CRCB) virtualization. Additional efficiencies include reduction in total time needed to process changes, a benefit provided by enabling the changing of approvers via smart phone. This feature shall facilitate approval of changes anytime, anywhere.

The Contractor IT Change Management Suite shall provide the County the option to create standardized and repeatable workflows. The suite shall include built-in best practices with associated industry-standard workflows, forms, and documentation. The suite shall create, modify, and reuse change processes, enabling continuous service improvements. With the Contractor IT Change Management Suite, different change types shall follow different paths. Pre-approved changes for standard requests shall be expedited while others follow a normal/conventional completion process. Scriptable and repeatable processes, including release management, provide the foundation for reducing risk and enhancing the benefits associated with change.

To help County visualize the end-to-end process, the Contractor IT Change Management solution shall provide a graphical workflow interface. The County shall be able to design, modify, and visually monitor multi-level processes. The solution shall expose every element of a change process—people, assets, timeframes, tasks, phases, and notifications—in clear, visual terms.

Through the Contractor IT Change Management Suite, the County shall be able to coordinate change activities across users and CRCB members, decision-makers, and other stakeholders involved with the change process. The County shall also be able to enable the suite to send automatic notifications to parties regarding potential changes affecting their respective systems.

The County shall additionally be able to assign, execute, and track CRCB action items, discussion threads, impact assessments, and voting. The Contractor IT Change Management Suite shall also automate potential collision detection, impact analysis, and risk assessments of change to the business. Moreover, the County shall be able to virtualize CRCB functions to enable decisions outside of actual meetings, increasing meeting effectiveness.

The Suite shall also include a global forward schedule of change that brings change requests together into a unified common view, providing improved visibility and planning. Change calendars shall be based on multiple views—including an Outlook-style calendar with timelines by month/week/day/hour, by application, and by implementer. This feature shall provide insight into the impacts, collisions, and comments of every change request. In addition, the Contractor IT Change Management Suite shall assign and track change windows, freeze periods, and business events, giving the County better control over when changes are implemented.

Contractor Service Manager solution and the Contractor IT Change Management Suite shall share configuration and dependency information found in an ITIL-aligned configuration management system (CMS) built on the Contractor's Universal Configuration Management Database (uCMDB). The Suite shall automatically and continually perform impact analysis, risk assessment, and collision detection on all change requests. Impacts and collisions shall be based on infrastructure and application relationships, but they can also reflect timing conflicts in personnel schedules (for example, the people responsible for implementing changes).

The Suite shall flag all impacted configuration items, potential applications, and associated business services using dependency mapping information. It shall also compare new change requests to all other pending requests within the same timeframe, and shall identify potential collisions that could result in downtime and rework. The Suite shall calculate a score based on multiple criteria—including historical outcomes of similar changes—for more accurate risk assessment.

As part of the overall Contractor's Service Manager solution, the Contractor IT Change Management Suite shall be tightly integrated with other ITSM processes and modules—from the logging of change requests through implementation, evaluation, and closure. This shall include integration with catalog, request, incident, problem, configuration, and service-level management components of Contractor Service Manager.

The companion Service Manager Service Catalog and Request Management modules shall provide integrated front ends into the change process.

Contractor Service Manager shall provide dashboards and reports that shall be easily customizable to provide managers and County leaders with quick and concise views into the overall status of the change process while enabling drill-down access to more detailed information.

The complete change process—from assembling requests through implementation and execution of change—shall be automated to speed the delivery time for standard change requests. Contractor shall integrate Contractor Operations Orchestration to enable faster RFC creation, change execution and provisioning, and closed-loop validation.

The Contractor Service Manager knows the "managed" state of configuration items (CIs)—or the state in which a CI is expected to be. The Contractor Universal CMDB with discovery and dependency mapping information shall maintain the "actual" states. After a change has been implemented, the managed and actual states shall be compared to validate that a change was successfully completed. In a similar manner, when a configuration item changes, the Contractor IT Change Management Suite shall compare this actual state of a CI against the record of change requests. Any change that does not have a corresponding change record shall be identified and addressed appropriately—by methods such as creating an incident or a new RFC.

The Contractor IT Change Management Suite shall enable Contractor and the County to establish effective IT process controls for change and configuration management. The built-in best practices based on ITIL shall align with common auditing frameworks such as Control Objectives for Information and related Technology (COBIT).

County involvement in the Change Management process.

All changes shall go through a formal change approval process as follows:

- When a change is desired, the change initiator shall complete an RFC ticket.
- The RFC shall be reviewed in the internal Technical Approval Board (TAB) review before it is released to County stakeholders.
- The RFC is submitted to the CRCB, which consists of both Contractor subject matter experts (SMEs) and County CTO representatives.
- The CRCB shall review the RFC and approve or disapprove the change.
- If the change is approved, the change initiator shall be notified as well as County end-users, and a Change Release shall be initiated.
- The Change Release shall be monitored through implementation and closure.
- A Post Implementation Review (PIR) shall be completed for each change at the completion of the RFC.

Metrics to measure the effectiveness of changes and conduct continuous improvement of the change management process.

Contractor shall continually assess these KPIs to identify negative trend lines. Contractor shall conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, thereby facilitating year-to-year continuous improvement.

2.14. Release Management Services

2.14.1. Process and Procedures

- Description of solution to meet the requirements

In practicing release management, Contractor shall combine the general business emphasis of traditional project management with a detailed technical knowledge of the system development lifecycle (SDLC) and ITIL practices. Contractor shall operate release management services in accordance with these practices, in complete transparency and collaboration with County stakeholders.

Solution: While the enterprise release manager on the account shall be responsible for tracking and logging all releases, the SDM for each business group shall perform this critical role. The SDM shall be responsible for understanding, monitoring, and assisting in the communication of these releases as they are completed in their respective business group.

In addition to the release review meeting that the release manager shall hold with the Contractor and County stakeholders, releases shall be reported in regularly scheduled meetings that the SDM shall be required to attend that fall within the scope of their duties. The SDM shall understand all information related to releases affecting their respective business group, bringing in SMEs if additional information is required.

Release management shall fall under the governance of the CRCB, which shall consist of both Contractor SMEs and County CTO representatives. All configuration items distributed into production shall use a formal release management process. Contractor shall develop a Release Plan that outlines the release schedule, content of the release, and back-out plans. Release management shall work with configuration management to make certain that the Definitive Software Library master IT configuration items remain current.

Rationale: The enterprise release manager shall be responsible for continuous improvement and shall work in collaboration with the County to facilitate the continued effectiveness of the process. Contractor's SDMs shall be responsible for understanding the releases and how they impact their respective business group. Contractor release managers shall be responsible for providing adherence to SDLC, ITIL, and Contractor best practices. They shall verify the completed release process is thoroughly documented and communicated to County stakeholders.

- Deployment plan for resources and use of facilities

The enterprise release manager shall work out of Contractor's Rancho Bernardo site.

- Key methodologies and processes in solution including year-to-year continuous improvement

The accuracy and diligence that Contractor provides in software configuration management (SCM) shall be realized by relatively issue-free releases, as Contractor moves into production and provide a stable, sustainable, and predictable release.

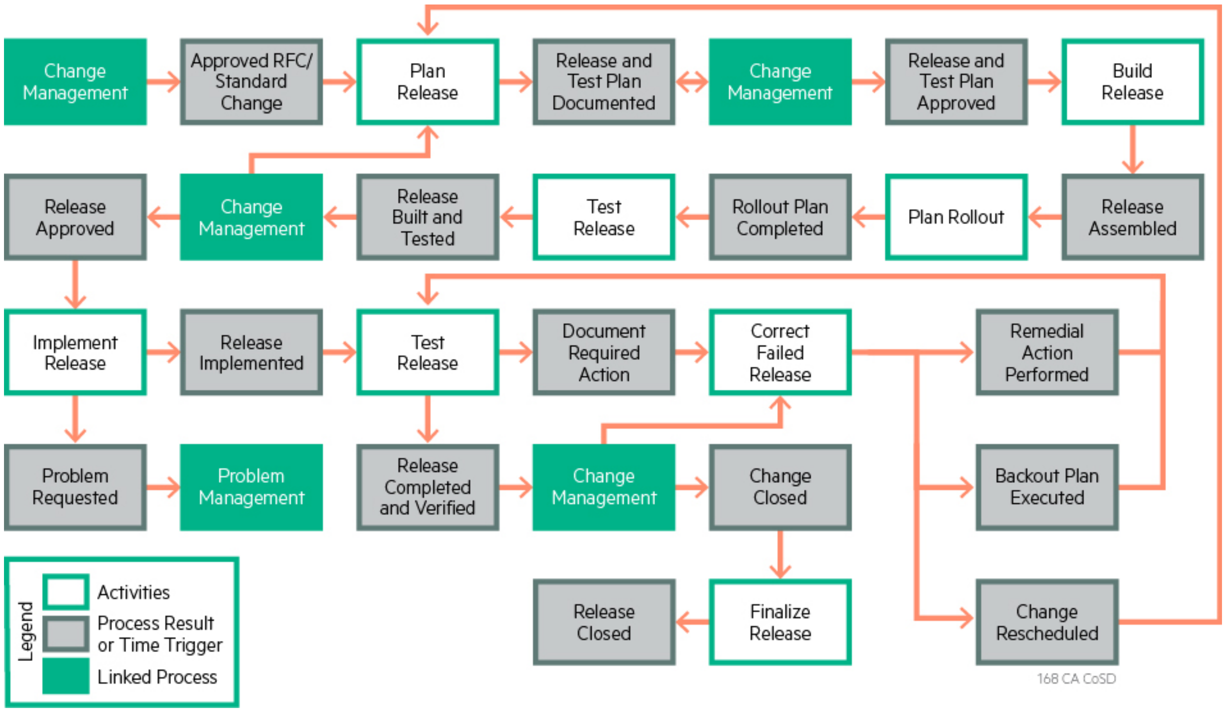
Release management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Its primary objective is to protect the integrity of the live environment and to make sure that the correct components are released.

Deployment is the activity responsible for movement of new or changed hardware, software, documentation, and processes to the live environment. The term "rollout" is most often used to refer to complex or phased deployments or deployments to multiple locations. Specific objectives of the process shall be as follows:

- Aligning, coordinating, and communicating release and deployment plans with County projects.
- Successfully building, installing, testing, and deploying a release package to the target environment along with the necessary documentation and training.
- Making certain that the new or changed service and underlying infrastructure are delivered to the agreed service level, providing the service utility, warranty, and level.
- Keeping to a minimum the impact on production services, operations, and support staff and business in general.

The following figure illustrates the Contractor standard release process.

Contractor Release Management Process



Proven process makes sure changes are effectively communicated, properly tested, and configuration controlled.

Contractor shall bring the change management process and shall align with and embrace the County’s release management policy.

2.15. Configuration Management Services

2.15.1. Process and Procedures

- Solution to meet the requirements

Configuration Management (CM) is the detailed recording and updating of information that describes an organization’s hardware and software. The tools are as follows:

- Apps Manager – Application related information
- Enterprise Server List (ESL) – data center hardware information (severs/storage/network/etc.)
- Asset Manager – Desktop-related asset information
- Endevor – Mainframe
- Serena – Archived source code related to applications
- Team Foundation Server (TFS) –Current source code solution
- AT&T data

Contractor shall adhere to the current Contractor-provided Configuration Management Plan, which supports/requires close customer collaboration and governs Contractor’s activities related to CM.

Solution: Contractor shall provide a Configuration Management System (CMS) and multiple CMDBs, accessible through the Service Portal that supports activities associated with recording, tracking, updating, and disseminating the County's configurations for all assets, including network assets. The CMS integrated across the organization and service frameworks shall support all logical configurations of hardware and software for the services. The CMS contains mappings to physical configuration, inventory data of hardware and software; Contractor shall use it to analyze trends as well as manage and reduce incidents and problems. The Service Portal shall display all information related to all assets from each tool mentioned above.

Contractor shall continue to provide software configuration management (SCM) via Apps Manager for the County of San Diego portfolio applications. Contractor shall make available the version control history as well as current versions of portfolio code and artifacts, including application code, software tools, and artifacts. Application SCM is part of the program CM and conforms to those policies and procedures.

Discrete item identifiers shall be associated with all configuration items (CIs). Applications' CIs include source code, compiled and/or linked code, packaged code, development environment tools, and any related documentation such as End-User manuals, test scripts, test results, project management documentation, architectural drawings, run books, and helpdesk scripts. Contractor SCM shall provide physical and logical online libraries for the CM of all software CIs. Contractor shall provide hardware-related information from ESL, which is where data center related equipment is tracked and controlled, and Asset Manager, which includes desktop-related hardware items. Contractor SCM is integrated with hardware configuration management data via a feed from ESL to Apps Manager.

Contractor SCM shall provide three libraries for applications code: two based on platform and one for vendor-delivered media. While Mainframe code resides in the legacy Endevor library on the mainframe, Windows and midrange code reside in TFS. More than a version control system, TFS uses a SQL Server database as a means of scaling to large environments and infrastructures. TFS shall be the key component in the life cycle platform, which enables third parties, customers, and solution providers to extend the base functionality with new features and customize the tool for unique County requirements and initiatives.

Contractor SCM shall manage third-party vendor code to include contracted code, public domain, purchased, and commercial off-the-shelf (COTS) packages. Third-party vendors shall use TFS for development of all applications CIs, unless a program-approved provision is in place for offsite development for that application. Third-party vendors shall make certain all code and artifacts are delivered in accordance with the Agreement. Contractor SCM shall review the third-party SCM practices and place the vendor deliverables under configuration management for the program.

Contractor and County-contracted third-party vendor code developed or maintained offsite shall follow County security and Contractor SCM standards. Purchased, public domain, and COTS software packages shall be implemented following County security requirements.

Rationale: Contractor's cross-functional configuration managers shall be responsible for understanding the interrelated and complementary CM requirements and best practices, and how they impact different frameworks and the greater IT organization. Cross-functional configuration managers shall be additionally responsible for making sure that proper communication and discussions for framework take place and that resources are available to manage and support all CM activities including reporting and portal accessibility by County stakeholders.

- Deployment plan for resources and use of facilities

CM personnel shall operate out of the Contractor's facility in Rancho Bernardo. AT&T personnel shall operate out of their facility on Trade Street.

- Key methodologies and processes in solution including year-to-year continuous improvement

Central to IT Service Management is a CMS and a set of core Service Management tools and databases that provide data to other ITIL or IT Service Management processes to deliver and support IT services throughout the County. The CMS comprises one or more CMDBs that collect and consolidate data from multiple sources into an aggregated view critical for timely and accurate decision-making.

TFS, for example, is a commercial software product specifically designed for CM administration that has been deployed at the County. All types of events that result in software or environment configuration changes shall be documented and tracked from initiation to closure.

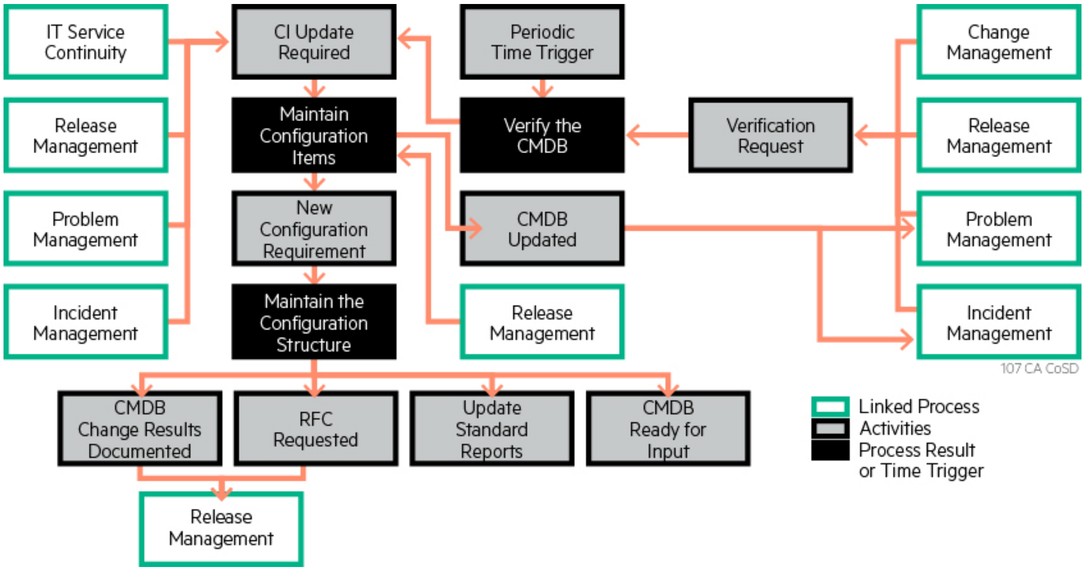
The primary purpose of CM at the County shall be to make certain that product attributes and technical baselines of all software and systems in use by the County—collectively known as configuration items (CIs)—conform to the documented design for each released software version. This shall include the means to document, track, and audit all design decisions and design modifications as well as software and environment build processes that verify the as-built software and host environments exactly match the intended design. CM is an activity that spans many groups across the organization, including management, requirements, process controls, tracking data, development, software tools, archival records, audits, and testing.

County CM shall include two primary teams that handle the bulk of the day-to-day CM tasks. Contractor shall perform this function and is primarily responsible for verifying that development proceeds according to the organization's documented CM rules. This group, with responsibility for the customized controls and rules, shall document and implement CM processes in a manner that is visible to all personnel; this group shall also make certain that released versions of County software products match the required and scoped content planned for that release. This group shall handle most CM status accounting functions and audit report functions, which are heavily automated through TFS. The second group is a development support team, whose duties shall include maintaining a fully versioned source code repository for each of the major County systems; developing automated build processes; building automatic installation packages; and providing software deployment across development, test, and production environments.

All modifications to this plan must obtain signoff by the County before going into effect. Additionally, quarterly quality reviews shall be conducted on the enterprise CM process, and results shall be reported to the County. Process End-User feedback and technology enhancement shall be used to continually improve the process.

The following figure depicts Contractor's standard CM process.

Figure 1. Contractor’s Standard Configuration Management Process



Delivering quality ITIL-based CM processes that the accuracy, currency and visibility of CIs

Solution for the integrated configuration management database that covers all Service Frameworks.

Contractor’s integrated CMDB shall record various CIs along with their attributes and relationships on behalf of the cross-functional service frameworks. Comprised of various framework CMDBs, the integrated CMDB and View shall be organized by framework and other key attributes. This shall enable individual CMDB CM administration as well as composite or service-wide CM. The Contractor configuration manager shall be responsible for the integrated databases.

Processes to maintain currency and accuracy of the integrated CMDB.

Contractor shall deploy auto-discovery tools to maintain accurate and current CMDB CI information.

Contractor shall proactively engage at all levels to make sure that the IT services it provides and sustains are optimal to meet the County’s current and evolving needs. Contractor shall collaborate with the County to provide and respond to the “over-the-horizon” view, which shall include at a minimum vigilantly monitoring asset inventories and software upgrades. Contractor shall make sure all iterations are captured and stored in CMDB and that County stakeholders are made aware of any anomalies or issues.

2.16. Capacity Planning and Performance Management Services

2.16.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor’s capacity planning and performance analysts shall collaborate with appropriate stakeholders in determining the resources required and make sure the performance or availability constraints shall not adversely affect County business. Response times and quality of services for End-Users shall be used as input and relevant data points to these decisions and performance assessments.

Contractor shall provide hardware, software, and configuration updates to servers, storage, desktops, and network so that the capacity maintenance and management is performed. The process shall involve the assembly of accurate reports of shortfalls, analysis of those shortfalls, and development of a solution to solve any capacity items that do not meet the goal. Contractor shall employ a cross framework process for ongoing proactive anomaly detection that involves representatives from all frameworks. The solution shall be implemented using existing data center procedures that may include County change approval. Virtual server implementation requires reconfiguration and can be done quickly, while implementation of physical servers may require the installation of new hardware, software, and/or configuration items. Changes recommended and approved shall be processed through the change process for implementation. After implementation, the responsible framework shall verify the effectiveness of the solution.

Contractor shall develop the Annual Capacity Management Procedures (ACP) as a key component of the Contractor solution. The purpose of ACP shall be to forecast County IT capacity and performance requirements on an annual basis and reaching forward. The ACP shall balance needs over the long term to optimize the resource workload expected in coming years. The primary inputs to the ACP process shall be historical performance information during the past year and the CTO technical roadmap, so that the forecast encompasses all data needed to meet immediate and extended future capacities and all service levels.

The output from this process shall be the projections for the next 2 years of IT capacity necessary to support the forecast, including identification of OS upgrades required to support the forecasted capacity.

The initiation of the ACP for report delivery to the County for review and approval shall begin during the mid-October timeframe.

The cross-functional capacity and performance management process shall assemble the prior year's historical information, including business forecasts, and shall generate the forecast during the planning period, including identifying OS upgrades if required.

The ACP shall be used to tune the performance management process for the new workload, and to selectively identify problems/opportunities that are to be undertaken as projects to mitigate some of the workload. The performance management process shall collect current system capacity and/or performance data and perform predictive analysis to identify the current capacity limits. This data shall be stored and used in annual capacity planning as historical information.

New desktop hardware technology shall be reviewed annually by desktop engineering. Capacity and performance specifications for desktop hardware and desktop applications in use or planned shall be reviewed with vendors to accommodate current and future County requirements and expectations. A report of recommendations shall be presented and reviewed with the CTO. The information collected throughout the year shall be incorporated into the ACP, providing adequate desktop services to maintain service delivery.

Rationale: Contractor's capacity planning and performance analysts shall be responsible for understanding the interrelated and complementary requirements, and how they impact different frameworks and the greater IT organization. In addition to discovering and analyzing critical touch points and KPIs, Contractor analysts shall thoroughly document and report their findings and activities and make the information available to County End-Users through the Service Portal.

- Deployment plan for resources and use of facilities

The positions required to provide capacity planning and performance management services are capacity planning manager and IT capacity planner. These personnel shall reside in Contractor's Rancho Bernardo facility. Network capacity planning shall be augmented by AT&T operating out of its facility on Trade Street.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor capacity management shall be an ITIL-compliant service that helps prevent business disruptions by proactively managing system use and capacity.

Contractor shall proactively and continually monitor capacity so that availability does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. Contractor shall also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies.

Capacity management shall make sure the County IT infrastructure is ready to meet the demands of users at agreed operational levels today and that IT services have the capacity to support future requirements. This shall be accomplished through collecting, analyzing, and reporting on capacity statistics and assessing the impact of County-planned projects. Contractor shall work closely with County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of infrastructure investments.

Contractor shall provide the County with data collected through automated reporting with an analysis of in-scope components' capacity consumption. A collection of reports shall display standard component utilization metrics, such as memory and CPU capacity.

Contractor shall group, and trend by day, all data for a single calendar month or monthly for the past 12 months.

County employees with access to the Service Portal shall be able to view the capacity reports at will, giving them the freedom to access data and reports as required. County employees shall be able to export reports to Adobe Acrobat, MS Excel, MS Word, or Rich Text format, enabling further analysis, combining with other data, or including in presentations and other documents.

Using automated scripts, Contractor shall extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, Contractor shall produce a forecast report using historical data that is trended over 12 months. Graphs include installed, usable, and forecast capacity data points.

The capacity management process shall rely on the key concept of a capacity management plan, which is a calendar-based data store that keeps track of workload identities, forecasts, and resource access quality of service requirements; resources that are associated with a pool; and assignments of workloads to resources. As a calendar-based data store, the plan shall keep track of such information as a function of date and time and uses it to support capacity planning.

"Configure resource pool size" shall be used to reduce capacity fragmentation by periodically repacking or consolidating workloads in a pool. "Find placement" shall balance loads, dividing them evenly across resources. It has two stages—if no resource is able to support the resulting capacity requirements, then Contractor shall attempt a larger scale rebalancing of workloads, adjust workload quality of service requirements, or combine the two approaches. "Add workload" shall report whether a placement can be found for a new workload.

Monitor, analyze and optimize capacity and performance in a virtualized data center.

Contractor shall provide capacity planning and performance optimizations as follows:

- Virtualization involves a different level of abstraction, where the relationship between shared resources is in a constant state of flux. Although enterprises view the supply side of capacity planning as pools or clusters of virtual resources, they must also understand which cluster or pool to use for an application and the broad impact on a virtual environment. For example, Contractor's virtualization specialists shall determine which clusters or pools need more resources as well as how updating virtual resources affects other resources. They shall make recommendations on how to deal with virtual machine (VM) sprawl (a proliferation problem), and when to reduce VM resources if Contractor believes they may be needed soon, but not currently.

- Although capacity planners have always been concerned about waste (or how much oversupply to have in reserve), the concept takes on new meaning in virtual environments, where the ease with which VMs and applications can be created has led to VM sprawl. Depending on the environment, waste due to VM sprawl can be considerable. Without proper insight into consumption requirements, enterprises risk vastly overestimating the resources needed to support their virtual environment.
- VMs do not exist in isolation; they run complex (often multi-tiered) applications that support many lines of business. Being able to profile how applications and business departments use (or potentially waste) the underlying physical resources is key. Even without a formal chargeback process, organizations need to understand how resources are being consumed so budget considerations can be calculated and sensible use of resources can be encouraged to meet demand.

Contractor VM specialists are experienced in VM environments and demand nuances, and share this experience and expertise with Contractor's capacity planning and performance analysts to make sure County virtual environments are accurately planned, used, and measured. Contractor shall proactively and continuously monitor capacity so that availability in the virtual environment does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. Contractor shall also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies. Should virtual capacity or performance require additional resources, Contractor shall immediately substantiate and initiate appropriate requests and notify appropriate stakeholders.

Once virtual environment considerations are factored in to the demand and use parameters of capacity planning and performance optimization, normal activities shall make sure the following occurs:

- Contractor shall use an ITIL-compliance capacity management service that helps prevent business disruptions by proactively managing system use and capacity. Making sure the right capacity is always available can mean increasing capacity based on County business and IT needs, or reducing or reallocating capacity so the County pays only for the hardware, software, and support needed.
- Capacity discovery shall occur through collecting, analyzing, and reporting on capacity statistics and assessing the impact of the County's planned projects. Contractor shall work closely with the County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of County's infrastructure investments, including people, processes, and tools.
  - Contractor shall extend this environment with sufficient capacity to accommodate increased workloads to include a new purpose-built Managed Private Cloud (MPC) environment. The MPC environment shall be a highly standardized environment with high-redundancy and scalability.
- Utilization reporting shall use data collected through automated reporting to provide an ongoing understanding and analysis of in-scope components' capacity consumption. A collection of reports shall display standard component utilization metrics, such as memory and CPU capacity. The lowest level of detail shall help with capacity planning and management.
- The capacity trend reporting feature shall provide more advanced reporting capabilities than the standard use report. Using automated scripts, Contractor shall extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, Contractor shall produce a forecast report using historical data that is trended over 12 months. Graphs shall include installed, usable, and forecast capacity data points.

- Use of Tools

The automated tool Contractor shall use to provide capacity planning is Contractor's Global Delivery Capacity and Performance Management (GDCPM) tool. This is a data warehouse that shall include database, storage, telecom, and networks. Other types of infrastructure data include system/server capacity management (forecasting and trending) metrics, availability metrics, and Performance management data.

2.17. Disaster Recovery Management Services

2.17.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor's DR management services shall provide strategy, process, type, methodology, locations, documentation, and prompt restoration of services. Contractor's solution is a subscription model, based on the County's specified Recovery Time Objective (RTO) and Recovery Point Objectives (RPO). Applications with a 72-hour RTO shall be recovered from replicated Virtual Tape Library (VTL) backups. Applications with a 48-hour RTO shall have their DR servers mounted to a replicated SAN storage. Under a subscription model, the server hardware "subscribed" to by the County is leveraged, provisioned with County images and applications on an as-needed basis to support DR tests, or actual disaster events. However, if shorter recovery times are required in the future, Contractor can implement active/active and/or active/passive-solutions, using dedicated server hardware, for web, application, and data layer recovery. License costs for active/active-synchronous, active/passive-asynchronous and active/passive vault tools are not included in base services.

During transition, Contractor shall validate ongoing DR policies and procedures including:

- Portfolio application priorities and Recovery Time Objectives/Recovery Point Objectives (RTO/RPO) requirements including:
  - Validation that restoration times meets County requirements
  - The server strategy (subscription using replicated backups or SAN data, or one of the dedicated hardware options above)
  - Data synchronization and replication plans
  - Rationalization of licensing costs.

The DR environments for the virtual servers within the MPC shall be virtual servers that spin up with a copy of the MPC virtual server.

Contractor's solution is based on F5 Global Traffic Manager (GTM) and Akamai. In in the event active/active, is implemented, Contractor shall support a synchronization technology such as SQL server Always-on architecture and Oracle Data Guard architecture. Contractor's technology Continuity of Operations (COOP) professionals, whose primary mission is to build a robust DR program for the County, shall write a viable and executable DR plan and schedule and manage DR exercises. Upon declaration of a DR event, Contractor shall execute the County Disaster Recovery Plan (to be developed during transition) that shall include:

Recovering and resuming full operations including all supporting infrastructure and networks in accordance with SLAs.

Rationale: Contractor's enterprise service delivery manager shall be the County point person and the conduit for information flow between remote disaster recovery managers and the County. Contractor's enterprise service delivery manager (ESDM) and remote DR managers shall be responsible for communication, managing resources, and supporting all DR activities, including during and after the event, which shall include a complete report to the County.

- Deployment plan for resources and use of facilities

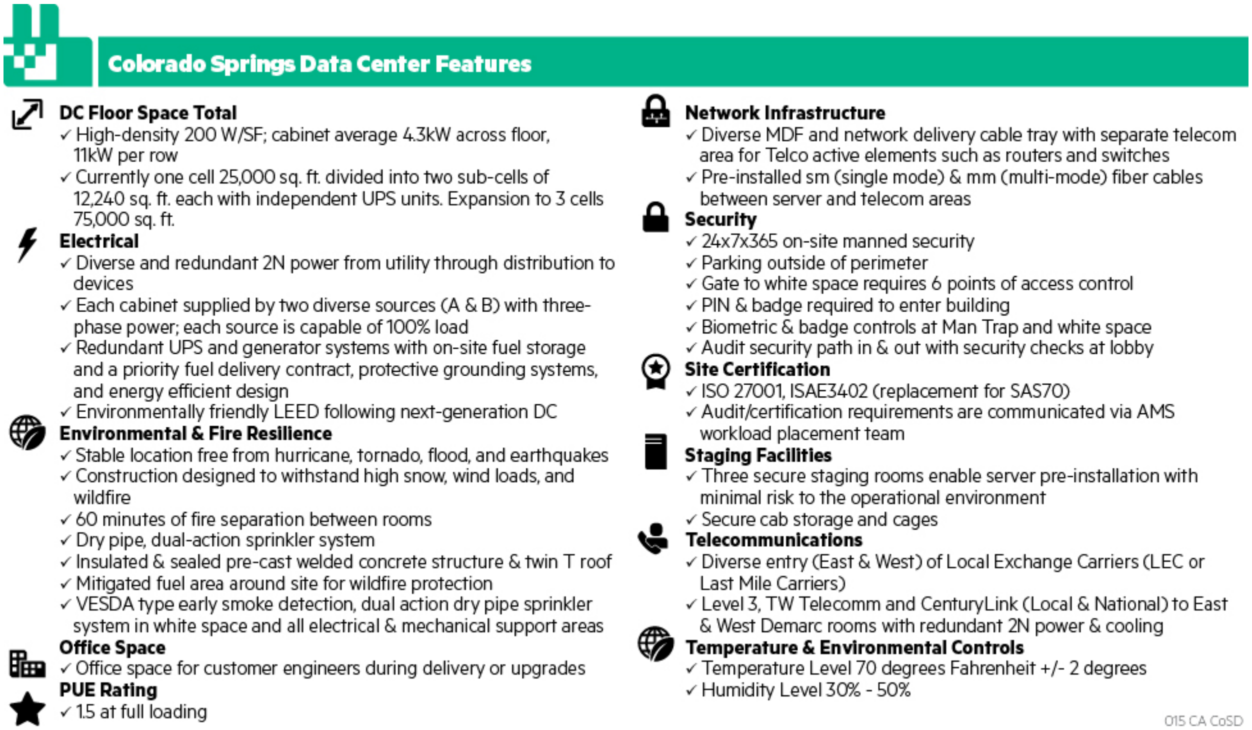
The County's recovery site shall be Contractor's Colorado Springs, CO Data Center (CSDC), connected via dedicated 10GB circuit, providing data replication. Contractor shall be able to provide a wide variety of disaster recovery services—dedicated to shared and/or hybrid solutions—at this central location.

Contractor shall write, maintain, and exercise County DR plans, and data center management professionals shall maintain the hardware, replication, and synchronization aspects of the solution. Connectivity and synchronization with CSDC shall include HPE's Tulsa production/development center and the County operations data center, as well as the AT&T POP, DR POP, Tower 9, Lemon Grove, and future sites as required. Coordination shall be managed by the Contractor ESDM.

The CSDC shall be a purpose-built, SSAE16-audited, data center. The Tier III data center design shall provide a completely redundant and continuously operating facility with infrastructure built with hot-swappable components, redundant power supplies and fans, compact flash, multi-boot support, and always-on management. Data synchronization and replication shall be determined by each application's RTO and RPO, and VM server versus physical server recovery methodology. Appliances shall be able to be deployed in traditional active/standby configuration or horizontal clusters (active/active) to achieve high availability and application-level failover. Contractor's CSDC MDRS facilities shall include locking cages, cabinets, and racks to meet County physical security requirements. This facility shall be used to provide DR and data backup services for Contractor's USPS clients as well as HPES Corporate.

Access to the CSDC shall be highly restricted. Access to network and Contractor computer equipment, storage media, critical support areas, and operations documentation shall only be granted to authorized personnel. Security consoles linked to alarm systems and closed circuit TV (CCTV) cameras shall be manned. Security cardkey readers shall protect all doors leading into the data center, and issuance of cardkeys for physical access to the facilities shall be controlled through a request and approval process. The following depicts features and capabilities of the CSDC.

CSDC Features and Capabilities



Colorado Springs Data Center Features

DC Floor Space Total
- ✓ High-density 200 W/SF; cabinet average 4.3kW across floor, 11kW per row
- ✓ Currently one cell 25,000 sq. ft. divided into two sub-cells of 12,240 sq. ft. each with independent UPS units. Expansion to 3 cells 75,000 sq. ft.

Electrical
- ✓ Diverse and redundant 2N power from utility through distribution to devices
- ✓ Each cabinet supplied by two diverse sources (A & B) with three-phase power; each source is capable of 100% load
- ✓ Redundant UPS and generator systems with on-site fuel storage and a priority fuel delivery contract, protective grounding systems, and energy efficient design
- ✓ Environmentally friendly LEED following next-generation DC

Environmental & Fire Resilience
- ✓ Stable location free from hurricane, tornado, flood, and earthquakes
- ✓ Construction designed to withstand high snow, wind loads, and wildfire
- ✓ 60 minutes of fire separation between rooms
- ✓ Dry pipe, dual-action sprinkler system
- ✓ Insulated & sealed pre-cast welded concrete structure & twin T roof
- ✓ Mitigated fuel area around site for wildfire protection
- ✓ VESDA type early smoke detection, dual action dry pipe sprinkler system in white space and all electrical & mechanical support areas

Office Space
- ✓ Office space for customer engineers during delivery or upgrades

PUE Rating
- ✓ 1.5 at full loading

Network Infrastructure
- ✓ Diverse MDF and network delivery cable tray with separate telecom area for Telco active elements such as routers and switches
- ✓ Pre-installed sm (single mode) & mm (multi-mode) fiber cables between server and telecom areas

Security
- ✓ 24x7x365 on-site manned security
- ✓ Parking outside of perimeter
- ✓ Gate to white space requires 6 points of access control
- ✓ PIN & badge required to enter building
- ✓ Biometric & badge controls at Man Trap and white space
- ✓ Audit security path in & out with security checks at lobby

Site Certification
- ✓ ISO 27001, ISAE3402 (replacement for SAS70)
- ✓ Audit/certification requirements are communicated via AMS workload placement team

Staging Facilities
- ✓ Three secure staging rooms enable server pre-installation with minimal risk to the operational environment
- ✓ Secure cab storage and cages

Telecommunications
- ✓ Diverse entry (East & West) of Local Exchange Carriers (LEC or Last Mile Carriers)
- ✓ Level 3, TW Telecomm and CenturyLink (Local & National) to East & West Demarc rooms with redundant 2N power & cooling

Temperature & Environmental Controls
- ✓ Temperature Level 70 degrees Fahrenheit +/- 2 degrees
- ✓ Humidity Level 30% - 50%

015 CA CoSD

Providing comprehensive, full-service data center capabilities that facilitate continuous processing and operational stability.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor’s DR program shall be built on industry best practices and standards of the Disaster Recovery Institute International (DRII) and ITIL. This model shall define four phases in the DR life cycle of a business continuity program—Analysis, design, build and integrate, and manage and evolve. The DR program shall include periodic and short-notice drills to validate the processes.

This model shall be flexible and adaptable, enabling phased implementation for the overall continuity program and for the County to enter and exit the life cycle at any point within the methodology process path.

The design phase is an enhanced DR (EDR) solution and the subscription DR solution for the 48- and 72-hour RTO systems respectively.

Contractor’s delivery team shall start with the build and integrate phase and stand-up the DR environment while Contractor continuity professionals begin the preliminary stages of drafting the DR plan. In this phase Contractor shall provision the replication circuit between the Tulsa data center and the CSDC recovery site. Contractor shall verify that data replication is occurring accurately and as planned. At the end of the phase, Contractor shall perform a tabletop exercise of the DR plan to validate its functionality and address any deficiencies found during the exercise.

At the conclusion of the tabletop exercise, the management and evolution phase of the DR program life cycle shall begin. In this phase Contractor and shall create and provide a master DR exercise calendar for County approval and work closely with the County to reflect the production changes into the DR environment in a methodical and timely manner. Contractor shall provide required training during this phase to make sure it is operating as expected.

In the analysis phase, Contractor shall work with County and assist in yearly undertakings such as a Business Impact Analysis (BIA) or identification of critical systems and apps. The following table outlines the features and benefits of Contractor’s approach.

Critical System Features

FEATURES	**BENEFITS**
CSDC Tier III, HPE corporate DR services, Federal DR clients, and is highly redundant and secure	• Highly skilled and experienced engineering, operations, security and program management resources • Experienced testing and compliance personnel
Network design that is redundant and secure, with automated GTM and load balancing capabilities with multi-layered firewall design	• Uses the skills and experience of Contractor’s network operations personnel • GTM automation works to reroute IP traffic in the event of a declaration • Automatic and transparent recovery and continuity of service

FEATURES	**BENEFITS**
Automated, continuous host-based replication for 48-hour RTO systems	• Automated, real-time maintenance of host images and data integrity • Near real-time RPOs • Can failover or fall back virtual-to-virtual or physical-to-virtual systems
Industry recognized DR PLANNING leader (Forrester-Traditional Disaster Recovery Service Providers)	• Highly skilled, trained, and BCM-certified personnel • Comprehensive development methodology • Experienced with Federal standards including NIST SP 800-34 Rev. 1
Continuous Process Improvement Loop	• Independent monitoring during exercises followed by after-action lessons learned to identify and integrate ways to improve DR processing

The DR plan shall be a cohesive document that includes an auditable overview, team structures, responsibilities, contact information, detailed recovery procedures, and recovery site activation aligned with NIST SP 800-34 Rev. Developed using Contractor templates, the plans shall be stored in a secure area of the Service Portal with access to authorized personnel only. Contractor shall design the plans to enable hand-off to County staff to complete its portion of the recovery and for data validation. Contractor shall also work with the County to create disaster definition and declaration processes relative to this proposal.

After approval, the DR plan shall be reviewed during an initial tabletop exercise. This exercise shall be conducted with County staff and operational leaders to fine-tune plan details and serve as a means to provide initial training to the County and Contractor. Additional training shall be provided to the County and Contractor delivery team as requested by the County.

As a standard operating procedure, Contractor shall incorporate client change management processes into the DR life cycle. Any change to the production environment shall be captured in the DR plan and the MDRS environment or it becomes impossible to maintain a viable and executable plan. Therefore, Contractor's lead continuity professional on the account shall be a member of the change control board.

Annual DR Exercises

Contractor shall schedule, plan, and lead one DR exercise annually in cooperation with the County. Contractor shall create and provide for County approval the strategy for the testing scope and a master schedule. Depending on various elements such as impact to the production environment or availability of the resources, exercises shall be live or table-top exercises. When possible, a DR exercise shall include an entire IT production site, or exercises shall be for all the applications in a given recovery tier or for a logical grouping of the applications. Contractor shall coordinate the following items:

- Laying out the entire exercise process with specific milestones, objectives, and metrics for each scheduled exercise
- Putting measures in place that track objectives

- Coordinating and preparing with the County application teams, users if desired, and any third-party vendors required
- During the exercise, measuring and tracking recovery timelines according to the County's RTOs and RPOs
- Documenting exercise results in a formal report, including comparison of the results to the measures and goals established, action items from the exercise, and recommendations on how the recovery process could be improved to be faster and more reliable
- Updates to plans as needed

County involvement with the Disaster Recovery plan.

County shall:

- Define RTO requirements
- Review/approve or disapprove DR plan
- Participate in drills and tests.

County Data recovery and restoration to meet the Service Levels.

For County data repositories restoration with no greater than a 28-hour data loss, Contractor shall provide data synchronization and replication that includes the County's immutable storage, live data, and virtual tape libraries.

For the systems and applications with a 48-hour RTO, Contractor shall use Contractor's EDR. This solution, which shall consist of replicating data center data asynchronously between the Tulsa production site and the CSDC recovery site, shall meet RTOs in as short as 4 hours.

For the systems and applications with a 72-hour RTO, Contractor shall:

- Deploy virtual tape libraries between the production and recovery sites, using the same replication circuit provisioned for EDR above. Contractor shall subscribe to physical or virtual servers for DR tests or during a true disaster event. Contractor continuity professionals shall stand up these servers within 12 hours of the disaster declaration, leaving 60 hours of the balance of the RTO to reconstitute the applications and data on the servers.

2.18. Identity Access Management Services

2.18.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall use IDAM technology to initiate, capture, record, and manage End-User identities and their related access permissions. Contractor shall make certain that access privileges are granted according to a singular interpretation of policy and that all individuals and services are properly authenticated, authorized, and audited.

Contractor's approach to provide IAM Services for the County shall be to:

- Enable the County to continue to execute its Identity Management Road Map
- Minimize risk and cost to the County by leveraging the County's current investment in Oracle IDAM platforms
- Build on the current Active Directory and Active Directory Federation Services (ADFS)
- Build on current PKI solution

All production servers, production storage, and Oracle licenses for the IDAM platform shall be provided through the applicable resource units and Third-Party Services.

The following table summarizes the billing approach for Identity Access Management Services (IAM):

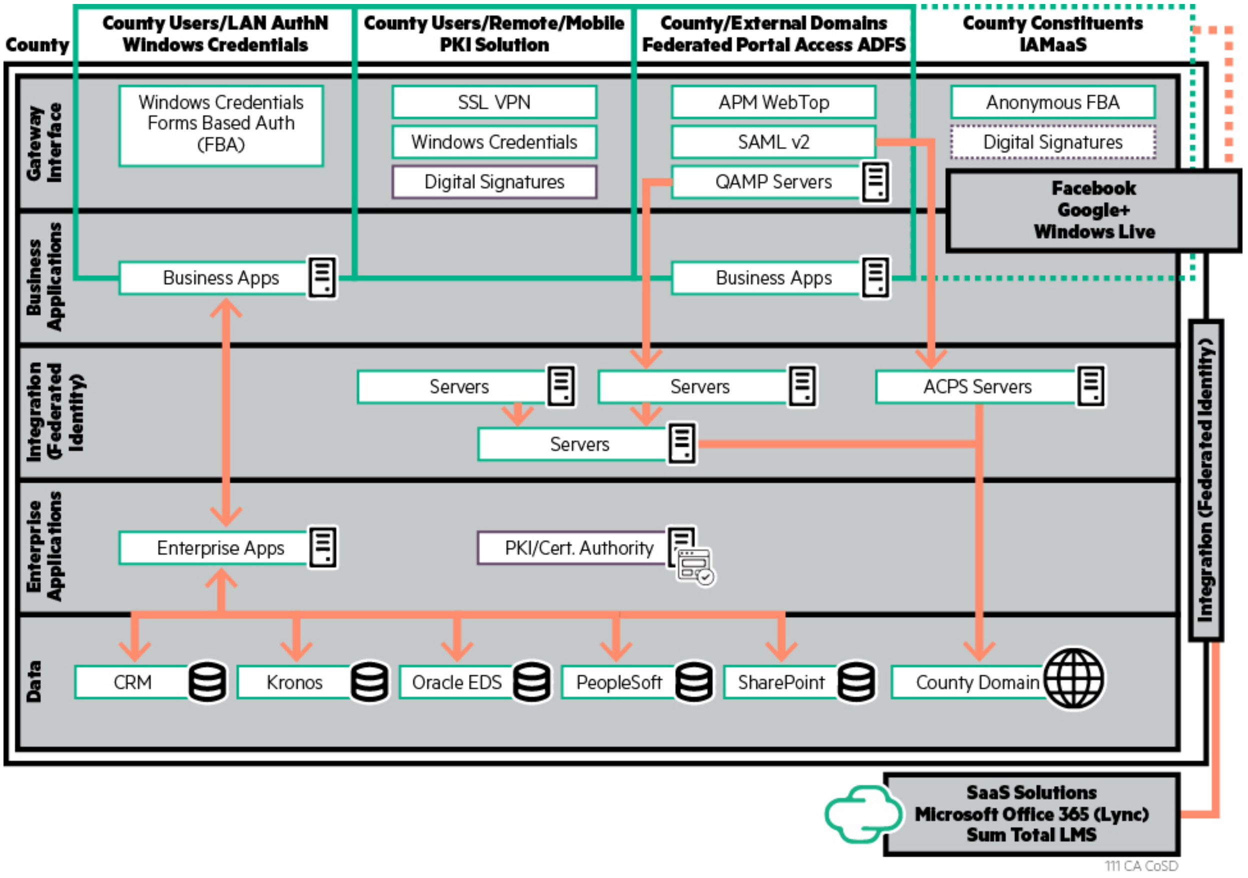
IAM Service	Hardware	Software	Support Labor
Active Directory (AD)	Infrastructure RU	N/A	IAM RU
Active Directory Federated Services (ADFS)	Infrastructure RU	N/A	IAM RU
Oracle Identity Access Management (IDAM)	Servers RU – Production Servers (County Responsibility)	Third Party Agreement (County Responsibility)	IAM RU
Public Key Infrastructure (PKI)	IAM RU (Luna Appliance Maintenance) Infrastructure RU (Servers)	IAM RU (certificate maintenance: 18,000 devices, 10 organizational, 16,400 user)	IAM RU
ID Provisioning	N/A	N/A	IAM RU

Solution: Contractor shall continue to evolve and improve the County’s existing investments in PeopleSoft, Active Directory (AD), and Oracle Identity and Access Management Platform (IDAM) to provide an overall platform to protect and manage individual identities, their authentication, authorization and roles, and privileges. The starting point or foundational element of the solution shall be the Oracle IDAM platform, which is an industry-leading, end-to-end security solution—providing components that protect applications, data, documents, and cloud-based services through a combination of flexible authentication and single sign-on, identity federation, and risk-based authentication and authorization. The IDAM solution—starting with the Oracle platform and extending to the current County Active Directory, PeopleSoft, Public Key Infrastructure (PKI), and Active Directory Federation Services (ADFS), shall provide an integrated, modular architecture. This architecture shall provide the County with the flexibility to deploy a complete solution that enables the integration of current platforms, existing applications, and third-party security services into a single solution—offered at a single price point.

The high-level scope of this solution shall be to use Oracle Identity Manager as the basis to manage the End-User accounts across various applications and integrate identities within Active Directory, PeopleSoft, and third-party applications that contain County identities. The Oracle Identity Manager shall act as a single point of End-User management for the administrator to create users and authorize the End-User to access the relevant resources across the County, while allowing the other key platforms that contain identities to continue. The Oracle Access Manager solution shall secure the application access with respect to organization applications. The figure below shows the main elements of the County Identity Management solution, which shall make use of existing capabilities while expanding the solution to meet all of the requested functions for the County. Depicted in the figure below are the four main “kinds” of identities that the County must manage/administer. These identities are as follows: “classic” referring to County users that exist on the County network, County users that are remote or “off-premise,” and County identities that require a federated relationship with external services such as County partners, residents or visitors.

By implementing the architecture illustrated in the figure below, each "kind" of County End-User shall be able to be managed in a low-risk, cost-effective, controlled, and secure manner so that management of the identities can be performed from a single point yet extend to each kind of End-User. Included in this solution shall be access to the County business applications, federation capabilities, enterprise applications, and County data sets.

- **San Diego County Functional Architecture**


County
County Users/LAN AuthN Windows Credentials
County Users/Remote/Mobile PKI Solution
County/External Domains Federated Portal Access ADFS
County Constituents IAMaaS
Gateway Interface
Business Applications
Integration (Federated Identity)
Enterprise Applications
Data
Windows Credentials Forms Based Auth (FBA)
SSL VPN
Windows Credentials
Digital Signatures
APM WebTop
SAML v2
QAMP Servers
Anonymous FBA
Digital Signatures
Facebook Google+ Windows Live
Business Apps
Business Apps
Servers
Servers
ACPS Servers
Servers
Enterprise Apps
PKI/Cert. Authority
CRM
Kronos
Oracle EDS
PeopleSoft
SharePoint
County Domain
Integration (Federated Identity)
SaaS Solutions Microsoft Office 365 (Lync) Sum Total LMS
111 CA CoSD

Providing secure IT services through comprehensive IAM.

This approach leverages the County's investments in Oracle, PKI, Active Directory, and ADFS; lowers the technical and operational risk by expanding on existing platforms; and enables the County to continue to execute its Identity Management Road Map and Strategic Plan.

The following Oracle elements are currently implemented within the County's IDAM Platform 11g Suite – IDAM Platform integrating them with Active Directory, PeopleSoft, and Contractor IAMaaS. The table below details each of the main elements of the integrated solution and what specific function they provide.

- **Solution Integration Components**

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
Oracle Identity Manager (OIM)	Integration with PeopleSoft	Onboarding for new employees Manage Health Care partners for Curam

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
		Provisioning applications users (Curam, EDPP, EBS, OBI, and other applications) Manage privileged accounts in AD and UNIX
Oracle Access Manager (OAM)	Provides Single Sign On (SSO) to 25 applications to County employees as well as firewall department users Federation with firewall department organizations as Service Provider	Continue to integrate more County-owned applications. Federation with third-party vendors as Identity Provider. Future capability to provide SSO capability to third-party vendor applications like Adobe Cloud, Adobe Analytics, LexisNexis, ABC Legal, Accurint, Attorney's Brief, Empinfo, e-Oscar, Inverify, Past-Employ, The Work Number, Westlaw, and Pacer. Future capability to provide risk-based multi-factor authentication capability for IDAM protected applications. Future capability to provide SSO capability to State-owned applications like CSE (CCSAS), CA Central, CALWIN, ECSS (State IVR), KidStar, and SAT C3.
IDAM architecture	Provide High Availability within one data center	Future capability to provide IDAM architecture as a Zero Downtime Architecture (requires re-architecture of the environment.)
IDAM Infrastructure monitoring	Monitor software components manually	Leverage licensed Oracle monitoring tool, Oracle Enterprise Manager (OEM), to monitor IDAM infrastructure (both software stacks and data base).

Contractor shall provide the following Identity and Access Management (IAM) Services as a component of the Cross Functional Framework and included in the IAM RU:

- Active Directory Security: provisioning of privileged IDs, service accounts, group policy and organizational unit management, synchronization service for Skype for Business and role based access implementation
- Midrange Security: provisioning of UNIX, local Wintel IDs
- Active Directory Federated Services
- PKI: Symantec PKI services for device certificates for laptops and mobile devices. Other devices shall be covered and included at the completion of Transition, at no additional costs, as per the Transition.
- Oracle IDAM platform (11g Suite):
    - Identity Manager, Access Manager, Internet Directory, and Virtual Directory integration with Active Directory and PeopleSoft.
    - Oracle Identity Manager integration with PeopleSoft.
    - Oracle Access Manager: federation with "Firewall Department" End-Users as well as Single Sign On to 25 applications for County employees and 'Firewall Department' users.

  - Oracle Federation Manager: Service Provider capability which allows the "Firewall Department" Users to utilize their own AD ID and password to access County applications via an interface with ADFS.
  - Oracle IDAM architecture: support high availability infrastructure within the Tulsa Data Center, scalable centralized directory service, manual monitoring of software components.

- Participation in architecture and strategy sessions with the County to advance and maintain the IAM roadmap

- Maintain the Identity Access Management Services Management Plan

- Maintain the Service Desk for all End-User IAM related Service Requests. Actions performed by the Service Desk are covered by the Service Desk RU; actions performed by IAM personnel are covered by the IAM RU.

- Ensure maintenance of overall security of the IAM solution, including adhering to County policy in the provisioning of IAM services and compliance with any applicable regulatory process

- With the exception for the server and storage costs, which are not included in the IAM RU, for all IAM supporting infrastructure, Contractor shall provide labor for break/fix, maintenance, availability management, patching, and IDAM activities resulted from hardware refresh.

- For all IDAM supporting software, Contractor shall provide point releases (e.g. x.1, to x.2), upgrades, and system documentation as part of the IAM RU. Contractor may require a Service Request for any work efforts in excess of $500,000.

Contractor shall provide integration of the PeopleSoft and Oracle Identity Access Management (IDAM) as part of the project in progress as of the CED titled "Automated Interface to PeopleSoft Application for IDAM Services." Part 1 is funded in accordance with the applicable Work Request and it is currently scheduled for completion in June 2017. Ongoing support for Part 1 and Part 2 for the resulting integration is included in the IAM RU.

Exceptions

The following services and related support shall not be included as part of the IAM RU, Transition or Transformation services.
These are either dependent on the implementation of other requirements, requires an assessment of line of business application compatibility to utilize the functionality, or fulfilled in conjunction with other requirements. These shall be part of the IAM Roadmap and require funding to design, implement and support.

- Additional use cases or additional applications for Service Provider and Identity Provider capability

- Onboarding additional applications to use enterprise single sign on functionality

- Onboarding additional applications to be provisioned via automated workflow process

- Consolidation of disparate End User accounts into IAM Implementation and related support of roadmap activities

- New functionality or services identified as part of future roadmap activities not already scoped in Transition

- Resource and Facility Approach Summary – deployment plan for resources and use of facilities

The Contractor team supporting the County shall work closely with the County CIO, CTO, and supporting staff and provide a close-knit working environment that allows for direct communication, service, and for the County to be able to reach out directly to Contractor for quick resolution of any issues. Contractor's Rancho Bernardo facility is the center of support for staff specifically assigned to support the County, and is the initial point of contact for the County for service. Other subject matter experts within Contractor's Identity and Access Management practice and portfolio virtual teams shall also provide support and service as needed. The Contractor's Tulsa Data Center in Tulsa, Oklahoma shall host the majority of County IT infrastructure and core IT services. This shall include the infrastructure for ADFS, Oracle IDAM, and Active Directory. The Contractor Continuity Services center in Colorado Springs shall be the designated disaster recovery (DR) site.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Key Processes

By incorporating the HP Global Method (HPGM) for Identity and Access Management, Contractor shall take an iterative approach, addressing issues and improvements in data quality and data management—in practice and in implementation. Through this process, Contractor shall work closely with the County data teams and other transformation, integration, and architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. HPGM for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology of "AgileFall."

In addition to HPGM Contractor shall also use a standard TOGAF-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is not only documented correctly, but also minimizes the overall implementation risk to the County. These methods shall be integrated with the County's current Architecture and Solution Reviews in conjunction with the County's CIO office and relevant County departments.

For the Oracle IDAM Suite, Contractor shall work with the current Contractor IDAM architect to make certain that the design, development, and deployment of the Oracle IDAM Suite follows standard Oracle design and deployment methods to make sure that the Oracle platform operates within the design parameters. Any significant design changes to the platform or changes to the Oracle Databases shall follow Oracle-mandated practices.

The Computer Services Registration Form (CSRF) and process shall be replaced to meet the County's requirement to develop automated workflows to manage access Service Requests. Contractor shall leverage the Oracle Identity Manager product to automate the Access Service Request process. Automation shall include the ability to create a request with all appropriate validations, route it for approvals, email notifications, and predefined reports. The Oracle access request feature shall integrate with the Service Portal as well as the automated provisioning capabilities that are specified in Schedule 4.3 Operational Services.

Any remaining requirements not in place at CED shall be included in the IAM roadmap.

Describe End-User account consolidation plan and End User Account Management Architecture.

Contractor shall develop a plan for account consolidation and management architecture as follows:

- Use the County Strategic Plan to provide the architecture vision for IDAM.
  - The County Strategic Plan is to build enterprise-grade identity and access. Re-architecting IDAM to become a Zero Downtime Platform to serve the application community is a future capability.
- Use the Oracle Identity Manager to manage all End-User accounts (expand existing capability via the "Automated Interface to PeopleSoft Application for IDAM Services" project stated above).

  - Currently, the County relies on the Computer Services Registration Form (CSRF) process and manual administration to manage End-User accounts. Contractor shall build a capability into Oracle Identity Manager that creates network and email accounts automatically when a new employee joins the County. It deactivates the accounts when an employee leaves, based on data fed from the County Human Resource System. Contractor shall build capability into Oracle Identity Manager so Contractor can manage Service Provider accounts.
- Contractor shall utilize End-User data within PeopleSoft to manage the life cycle within the Oracle Identity Manager (via the "Automated Interface to PeopleSoft Application for IDAM Services" project stated above).
  - Use PeopleSoft to determine the life cycle of an ID.

    When a new employee joins the County, the Human Resources system shall be the authoritative source for identity data. For the County, this is its PeopleSoft (PSFT) application, which shall have a record for each employee. Oracle Identity Manager (OIM) shall be integrated with PSFT, and when a record is provided for a new employee, then OIM shall create accounts automatically in the County's Active Directory and Exchange environment. When an employee leaves the County, PSFT shall indicate such activity, and OIM shall inactivate the corresponding accounts in AD, Exchange, and other End-User stores. When an employee transfers to another department or business organization, then OIM shall receive notification from PSFT and take action based on established business rules. As the authoritative source of identity information, PeopleSoft shall be the driver of any necessary actions by OIM, and the process shall be automated with little need for manual administration.

  - Actions taken on the County End-User accounts shall be based on business rules established within the County such as hire, termination, transfers, leave of absence (LOA)/return from leave, and re-hire.

    As described above, PeopleSoft shall be the driver of the actions taken by OIM. Although the actions taken by OIM are triggered from PeopleSoft updates, the actions themselves shall be directed based on business rules that can be integrated into OIM. For example, if the trigger from PeopleSoft is a transfer between one department to another within the County organizations then rules can be programmed into OIM that would disable access to one type of data and allow access to other data if that was the policy. In the case of a termination notification from PeopleSoft, OIM would disable Active Directory and Exchange accounts.

2.19. Reporting Management Services

2.19.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall develop, generate, and submit deliverables. Contractor knows the current reporting criteria and shall continue the current level of reporting without interruption upon Transition completion. Contractor shall identify necessary reporting additions and enhancements to be completed as part of the overall cross-functional transition timeline. As part of the transition process for each framework, Contractor shall develop that framework's new report set (as identified in the RFP), either as a new report, or as an update to an existing report, where applicable. As the new reports are completed, Contractor shall begin posting them on the Service Portal. During the Cross-Functional transition, Contractor shall also implement Microsoft SQL Server Business Intelligence to begin the process of the data warehouse development. The data warehouse shall provide a central repository that supports other analytic scenarios as determined by reporting and County/Contractor quarterly review. Contractor is committed to continuous improvement and, over time, Contractor shall work with the County to extend both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured through increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

Specific areas of ITSM that can benefit from analytics:

- Service Strategy and Improvement Analytics: This area shall focus on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Service Operations Analytics: Blending ITSM data and baseline IT performance data, Contractor shall conduct analyses to reduce business impact of events, incidents, and problems.

Post-transition, through a coordinated effort, Contractor shall identify specific subject matter experts for each reporting requirement and match them with a County counterpart to make certain that any new requirements are identified and supported for each of the Schedule 5 reports. In addition, Contractor shall demonstrate new and additional reports that the County finds valuable to manage their IT infrastructure, as well as streamline the reporting process as new transition and transformation tools are applied. The County shall have near-real-time reporting with fresh data to proactively monitor service performance and to take necessary actions. Service Manager provides 100+ out-of-box (OOB) reports; intuitive UI helps to create easily navigable role-based dashboards to show only what is applicable to a particular role. Each report shall have the option of printing and exporting (PDF, MS Excel, and HTML). Service Manager also has built-in reports for KPI reporting.

Rationale: Contractor shall have a well-documented and dynamic reporting management operation. Contractor's data analysts and Cross-Functional leadership shall be responsible for making certain that reports are generated accurately, on time, and in accordance with design or agreed-upon specifications.

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The County shall continue to receive the current reports during the transition period. Contractor shall work with the County to consider new and improved reports through conducting workshops and meetings for the County to consider modifications to existing reports or to make new reports. These collaborative sessions shall be conducted by Contractor resources at its facility in Rancho Bernardo or at County sites identified by Contractor's customer.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall provide to the County all reports via the Service Portal. Contractor shall provide these reports and track the usage to provide feedback to the County on reports in high demand and those that potentially could be modified to provide additional value or possibly sunset.

Contractor shall create an analytics and reporting data warehouse during the transition period, based on MS SQL Server Business Intelligence, to facilitate ongoing automation and continuous improvement in efficiency and quality of Contractor's reporting capability.

- Use of Tools

Contractor shall use tools and data extract processes in the course of producing reports. The appropriate tools and products to be used in producing each report shall be finalized during the transition period, but shall consist of, at a minimum:

- Microsoft SQL Server Business Intelligence
- Microsoft SharePoint
- Contractor End User Access (Service Portal)
- EMC Documentum (DocVault)
- Various scripts and development tools, as appropriate

2.20. Domain Name Management Services

2.20.1. Process and Procedures

- Solution to meet the requirements and the rationale

Solution: The request for a new Domain Name (DN) and add-on DN services shall be initiated by the County point of contact (POC) via an IMAR request to the Contractor Service Desk or a project requirement. The Domain Name Administrator (DN Admin) treats either request as authorization to purchase the DN and DN services from an accredited registrar/vendor.

The Contractor Service Desk routes the IMAR request to the DN Admin, who takes the following actions:

- The DN Admin shall check the DN Portfolio for an existing account for the requesting department. If the requesting department has an account, then the DN Admin uses the existing account for purchase or creates a new account if one does not exist.
- The DN Admin shall save the confirmation receipt for future reference and adds DN and DN services to the DN Portfolio in the Integrated Asset Management System (IAMS).
- The DN Admin shall then email the County POC the confirmation of purchase and gives the County POC an initial username and password.
- If the requested DN is not available, the DN Admin shall email the requestor for an alternative DN.

The DN Admin shall be responsible for (1) actively monitoring the renewal of DN and associated DN services and (2) acquiring approval from the County POC for renewal. The DN Admin shall take the following steps for renewal:

- The DN Admin emails the County POC about DN renewal approximately 30 days before the expiration date. If there are DN services associated, then the DN Admin also requests DN services renewal.
- The County POC responds with approval to renew the DN. If there are DN services associated, the County POC also indicates whether or not to renew the DN services.
- The DN Admin pays renewal fees to the accredited registrar/vendor for the DN.
- The DN Admin updates the expiration date on the DN Portfolio accordingly and enters it into the IAMS.
- If the County POC decides not to renew the DN then the DN Admin updates the DN Portfolio in the IAMS.

The County POC may request cancellation of a DN and associated DN services prior to its expiration. The DN Admin shall treat these requests as authorization to release the DN and associated DN services. The following are the procedures for cancellation of a DN:

- The County POC submits an IMAR-Remove ticket in myRequests.
- The Service Desk routes the IMAR-Remove ticket to the DN Admin.
- The DN Admin cancels the DN and associated DN services with the registrar/vendor, removes the DN from the DN Portfolio, and saves the documentation in the IA.

The DN Admin minimizes the number of registrars/vendors from whom they purchase DNs for ease of management and transition of services. The DN Admin shall purchase/renew DNs for no more than a 1-year subscription to minimize the cost to the County in the event that a cancellation occurs. Contractor shall consolidate domain names to only accredited registrars, as each DN comes up for renewal.

The DN Admin shall create an Annual Domain Name Management Plan that details all DNs in the DN Portfolio, expiration dates of existing DNs, and any changes in DN management procedures. The DN Admin shall also create and post to the Service Portal a monthly report that shall include the following:

- Domain Name
- Total quantity of managed Domain Names
- Quantity of new Domain Names added in the last month
- Quantity of Domain Names retired in the last month
- Quantity of Domain Names retained by the County
- Summary data for each Domain Name:
  - Domain Name ID
  - Type/extension
  - Renewal date
  - High Org
  - Low Org
  - County POC name, email, and phone
  - Secondary County POC name, email, and phone.

Contractor shall provide Domain Name Management Services is for unlimited number of domain names.

- Deployment plan for resources and use of facilities

Domain Name management is performed by Contractor's Domain Name Administrator, who shall reside in Contractor's facility in Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall conduct the Domain Name management in accordance with the agreed-upon Domain Change Management process with the County. Contractor shall implement continuous improvement in accordance with the Contractor's ISO 9000-certified processes and Contractor's adherence to ITIL processes for service delivery, including the review, analysis, prioritization, and recommended improvement opportunities.

The Domain Name Portfolio shall be stored and continually updated in the Integrated Asset Management System.

2.21. Business Analyst Services

2.21.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall establish a team of business analysts. These analysts shall create, gather, analyze, communicate, and validate requirements related to new IT projects or changes to existing applications, processes, or policies. The Contractor business analysts shall engage all County and Contractor stakeholders as well as contractor roles across the applications, engineering, testing, End-User support, and security towers. Contractor's solution recognizes the complexity of this role and provides tools for multifunctional teams.

Contractor shall work closely with the County business owners and users. Business analysts have an advanced level of knowledge and expertise within the particular industry or client they support. Contractor shall field a mix of experts who know the County’s business well and are strong in eliciting and documenting requirements. This hybrid approach to staffing the Business Analysis Center (BAC) gives the County the optimal mix of knowledge of its business and functional/technical expertise from outside the County. The implementation of the BAC shall include:

- Flexibility in the business analyst staffing arrangement. - Analysts shall be available through a pool of resources the County can use on request or exclusively for specific projects or objectives.
- Shorter delivery time to meet customer demands. - As the County has direct contact with Contractor business analysts that can act as a bridge between requirements definition and solution development, it can improve and enhance service delivery to its employees and constituents.
- Experience in aligning the right resource to the right effort. –Contractor’s solution for business analysis focuses on the identification, training, and development of experienced business analyst professionals.
- Quality and standardization in requirements identification and development. – As part of the BAC, each analyst benefits from a common set of industry standard best practices as defined by the BAC and approved by the County. These processes shall not only define behaviors and methodologies for assisting the county to develop the quality SOWs and requirements documents that are necessary to expedite project outcomes but also to create a smooth transition from identification of business needs through the project request process, requirements development, and beyond.
- Continued engagement throughout the project life cycle. - Business analysts shall participate in post-requirements phases, for example, guiding End-User acceptance testing and acting as training and documentation SMEs.

To support the solution, Contractor shall leverage its Enabling Delivery and Global Excellence (EDGE) methodology and toolset to develop the standard processes the team shall follow. EDGE is a repository of best multifunctional methods, tools, and processes that inform the creation of a custom, repeatable solution.

Rationale. Contractor’s executive leaders are advocates of continued and expanded business analysis support.

Business analysis services shall meet the following objectives:

- Support the County by increasing the maturity, consistency, cost-effectiveness, and overall business value of business analysis services by developing a BAC
- Provide the right mix of County business knowledge, technology expertise, and business analysis expertise
- Provide a methodology and tools with flexibility for all types of projects, regardless of size or complexity
- Provide access to embedded business analysis resources via the BAC
- Provide portal-based access to a business analysis methodology tailored for the County
- Assist with business analysis training for County users via the BAC. This training shall be focused on project-specific needs
- Keep all processes lean and responsive to the County without creating too many procedures for business analysis to allow for expedited delivery
- Provide business analysts with the right aptitudes, certifications, and ongoing training.

- Deployment plan for resources and use of facilities

Contractor shall provide a pool of business analyst resources to be guided by common and flexible best practices and tools, which shall improve the quality standard for requirements gathering.

Contractor shall be flexible when assigning the work locations of all analysts to meet the needs of the projects and departments. Analysts shall be located in either the Contractor’s Rancho Bernardo facility or an embedded location within the County. If a County department wants a dedicated resource, Contractor has that flexibility and shall work with the County to identify the best resource and solution.

Following Contractor's flexible, hybrid approach, Contractor shall provide an opportunity for current business analysts to gain more training and certifications as part of their professional development. Contractor shall develop talent and enhance staffing where necessary to meet the County's needs. In addition, Contractor requires specialized business analysis training, experience, and certifications when engaging new talent. Incoming business analysts shall demonstrate at minimum:

- Business- and technology-related education and experience
- Professional experience performing business analysis services
- Exceptional communications skills and strong interpersonal skills, including structured and unstructured facilitation
- Ability to understand and document functional business requirements and to translate business requirements into technical requirements and/or solutions
- Experience with formal business analysis methods and tools
- International Institute of Business Analysis (IIBA) Certified Business Analysis Professional™ (CBAP) certification or similar is a plus.

- Processes in solution including year-to-year continuous improvement

Contractor shall publish a County business analysis methodology on the Service Portal and use the BAC to help use and extend best practices throughout all County projects.

Enterprise-Level Best Practices

Contractor's first three best practices shall be implemented at the enterprise level. Through enterprise-wide standardization, a common language, and traceability, the County can create well-defined requirements that provide consistency throughout the application life cycle and become part of the County culture.

Enterprise-wide standardization - By standardizing requirements management at the enterprise level, the County can promote collaboration and eliminate silos between business analysts, development, and quality assurance (QA). A single system for complete requirements management provides the most up-to-date information for project teams. This is particularly important as requirements change over time, either because of changing business conditions or by design as part of an iterative development process such as Agile. A single requirements management system also enables better oversight.

Common language - Providing consistent guidelines for the language used for all requirements makes requirements easier to write and follow. This prevents both the overwork of adding more detail than necessary and the extra time needed to cycle back for more information when descriptions are too vague.

As a guideline these quality metrics include:

- **Lines of text**—the number of lines of text in the requirements document. When there is uniformity in the way requirements are described, this metric allows the End-User to estimate the functionality and degree of testing required for the software.
- **Imperatives**—the number of imperatives in different categories, such as "shall," "must," This number gives a rough estimate of the degree of design functionality required in the software. It also gives an estimate of the degree of testing required to satisfy these imperatives.
- **Weak phrases**—the number of weak phrases such as "large," "fast," "enough," etc. Weak phrases indicate vague design requirements that are non-testable.
- **Completeness**—the percentage of requirements that do not contain phrases such as "TBD" (to be determined) and "TBS" (to be specified). Requirements containing these phrases are considered incomplete.
- **Option phrases**—the number of phrases such as "can," "may," "I/we think," and so forth. These indicate requirements that might be difficult to satisfy in development.

Another best practice to encourage the use of a common language for requirements is to provide a template or set of templates for requirements definition.

Traceability - Contractor shall enable traceability throughout the application life cycle to determine whether a project meets requirements. The ability to bi-directionally trace links between requirements and testing.

Traceability metrics include:

- Requirements traced —number of requirements traced to or from each specification
- Requirements untraced—number of requirements that are not traced
- Requirements inconsistently traced—number of requirements inconsistently traced
- Linkages—number of upward and downward linkages for each requirement. This helps determine reuse and the impact of changes on the overall application
- Coverage—percentage of requirements traced to passed tests, failed tests, or tests not run.

Project-Level Best Practices

The next four best practices occur at the project level. Adopting these practices brings clarity to the requirements process and helps eliminate rework in application development and testing. In addition, these steps help eliminate overwork and rework in the requirements definition process itself.

Be lean. Do not create requirements assets unless they provide value to the application team. The assets with the most value are the ones that can be reused. A lean approach includes automating processes and eliminating waste. By systematically organizing requirements, it becomes easier to see which requirements are needed and which can be eliminated. Standardizing the content of requirements—with templates and a common language—helps make requirements easier to understand and eliminates rework.

Iterate. Create requirements iteratively to generate feedback, promote collaboration, and enable teams to identify defects early in the software development life cycle. A best practice is to start with a high-level business requirement by describing who needs the functionality for what purpose and why. Then, rather than working in isolation, the business analyst writing the requirement gathers feedback from major stakeholders on whether the high-level requirement adequately describes the business need. Developers also provide feedback on whether there is enough information to begin coding. If not, the business analyst drills down to add more detail. If there is enough information, the developers can get started.

Different requirements require different levels of detail. The County can save time and reduce complexity by providing just enough elaboration. There is no need to over-describe requirements that are easily understood.

Requirements assets that can be reused, such as business process models (BPMs) that can be used to generate requirements, provide the most value.

As a project goes through iterations of requirements definition, it is important to measure where and how requirements change over time. Change metrics include:

- **Volatility**— number of requirements added, deleted, and modified, classified by a reason for change.
- **Initial allocated requirements**—number of technical and nontechnical requirements originally provided by the customer. This metric, along with final allocated requirements and changes per requirement, describes how much requirements change.
- **Final allocated requirements**—number of technical and nontechnical requirements that were used to build the final software product.
- **Changes per requirement**—number of changes made to each requirement.
- **Changes over time**—number of changes per week, for example. This describes the degree of requirements volatility. This number decreases towards the end of the software life cycle, indicating convergence of requirements.

- **Cause of change**—categorizing the cause of changes helps in identifying the most common reasons for change and can be used to improve the software process.
- **Source of change**—identifying the source of change (that is, who requested the change) helps anticipate the sources for change in the future.

Visualize. Contractor can use visualization to increase understanding of requirements and the dependencies between requirements. Visualization makes it easier to identify potential problems, such as missing use cases. And pictures can be easier to read and navigate than text-based requirements. For teams that do not want to follow the Agile practice of writing code early in the process, visualization and simulations can be used to elicit early feedback to achieve many of the same objectives.

Collaborate. Collaborate and break down silos between groups from the beginning of the process. For instance, while a business analyst might have the End-User view of what a requirement should be, collaborating with the development team helps determine whether implementation of the requirement is feasible.

When these best practices are implemented, Contractor projects are more likely to meet intended business metrics, including budgets, schedules, and client satisfaction by eliminating the gaps between work processes performed in IT silos.

Standardization and Best Practices.

Embedded in Contractor's methodologies are common best practices that can be tailored to suit the County's needs, including those from BABOK, CMMI, ISO, and SSE. These methodologies integrate business analysis with the other development disciplines to verify continuity of standards through the project stages.

Gather and document County business functional requirements when working with County departments.

Contractor shall leverage its Enabling Delivery and Global Excellence (EDGE) methodology and toolset. EDGE is a flexible repository of best multi-functional methods, tools, and processes that Contractor shall tailor for each County project.

Contractor Business Analysis Services relies on a set a proven best practices, but is highly flexible for the County. Contractor shall draw on a pool of business analysts who have a mix of experience and diverse technical expertise and functional knowledge of the County and its businesses. The analysts shall work directly with the County user groups to accomplish the following:

- **Gain Broad Involvement**. Review documented high-level requirements with internal stakeholders, including representatives of those capabilities who shall be responsible for delivering the solution.
- **Define Goals and Requirements**. Confirm that defined detailed requirements support the business goals and provide compelling business value. Reconfirm boundaries for: business functions, current systems, internal and external interfaces. Confirm stakeholder and End-User profiles, business processes, End-User interfaces and use cases, interface requirements, business rules, data entities, non-functional requirements, geographic regions, language/culture considerations, volumetric(s) (e.g., how many reports were anticipated), and documentation.
- **Define Scope**. Identify perceived gaps in boundary definitions as issues. Document questions and assumptions with regards to understanding the high-level requirements. Transfer knowledge of detailed requirements and estimating assumptions (if any) from solution architect to business analysts and project team.
- **Use Leverage**. Leverage the experience of the detailed requirements development team and transfer knowledge to the solution delivery team. Review assumptions and constraints. Identify perceived barriers to evolving the detailed requirements into a solution. Confirm common understanding of the detailed requirements with client stakeholders. Review and discuss gaps, issues, questions, concerns, and assumptions.

- **Build Consensus**. Determine if the client and project manager agree that the detailed requirements are sufficient for solution development. If the detailed requirements are not sufficient, work with project leadership to assess the impact of delays resulting from rework of the high-level requirements. Raise requests for change as needed
- **Document Results**. The output of this work is a Business Functional Requirements Document. Once the functional requirements are agreed on, documented, and approved by the County, they can be translated into technical requirements or directly into a solution depending on the complexity and functional nature of the requirement. Contractor shall use templates that are already in use with the County and supplement them as needed with best practices templates from EDGE.

With this process and approach, the County users are involved every step of the way and own approval of the final Business Functional Requirements Document as the baseline for next steps in implementing a solution.

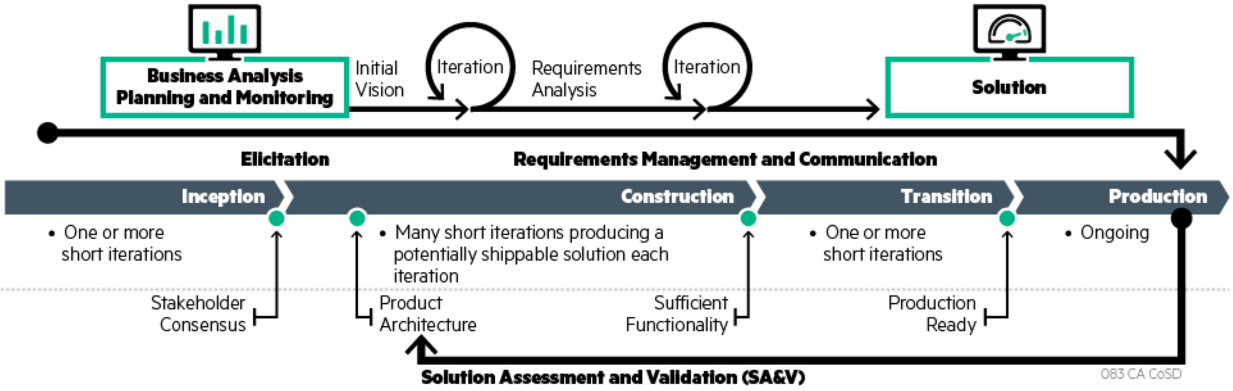
Translate business requirements into solutions or technical requirements.

Contractor's Business Functional Requirements Document shall include:

- Review Functional Business Requirements and confirm joint understanding of the requirements (this process is streamlined and low risk if HPE business analysts helped develop the functional requirements.
- Assess functional requirements and technical components required to meet requirements
- Map all functional requirements to technical requirements
- Ingest and consider technical alternatives and review with the County
- Make build versus buy decision and gain County approval
- Iterate technical specification and solution versus functional requirements to optimize business case – discuss tradeoffs with users and gain their approval
- Perform SIT and UAT
- Deploy

Contractor has a comprehensive process for this translation and solution development, as illustrated in the following figure:

Process to Translate from Requirements to Solution


Business Analysis Planning and Monitoring
Initial Vision
Iteration
Requirements Analysis
Iteration
Solution
Elicitation
Requirements Management and Communication
Inception
Construction
Transition
Production
• One or more short iterations
• Many short iterations producing a potentially shippable solution each iteration
• One or more short iterations
• Ongoing
Stakeholder Consensus
Product Architecture
Sufficient Functionality
Production Ready
Solution Assessment and Validation (SA&V)
083 CA CoSD

Contractor shall provide a streamlined approach to reach a solution provides sufficient process control to achieve success.

Additionally, Contractor use the following best practices when translating requirements into solutions:

Once requirements are developed and refined, Contractor and the County may also conduct a Build versus Buy Analysis that identifies a "best-fit" solution based on requirements and budget. The best return for the County comes when business requirements, staffing, and technology are optimally aligned with both End-User and mission needs. The business analyst's job is to analyze needs, document requirements, and identify optimal solutions.

Build. Contractor shall execute the requirements elicitation approach identified in planning until sufficient information is gathered to document the detailed requirements and estimate the cost to build. This cost can be compared to cost to buy COTS, and a final build versus buy decision is made. Contractor shall refer to previous iteration/release documentation as needed to shape the scope of the detailed requirements elicitation.

Depending on the nature of the build, Contractor shall decompose high-level information; abstract low-level information; distinguish requests versus needs; and distinguish requirements from design constraints. Identified requirements shall include functional/system requirements and may include non-functional requirements (such as performance, environmental, security, etc.), service-level requirements, quality requirements, and project management-related requirements deemed critical for project success.

Contractor shall store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference. Contractor shall document the decision criteria and justification for selecting the build option. Contractor shall select a build process, which leads to a build or development phase.

Buy. A COTS solution may be the lowest risk and least costly way to meet End-User functional requirements.

Contractor shall validate high-level requirements against the selected COTS product and perform a detailed assessment of the gaps to confirm that the essential requirements can be met (out-of-the-box, by configuration, or by customization). Business analysts shall be trained in the use of the selected product (including the features, flow, and architecture) or Contractor shall include COTS SMEs in the elicitation activities to clarify how the COTS product can meet the requirements or the impact of potential customizations.

Contractor shall store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference Contractor shall document the decision criteria and justification for selecting the buy option.

Ensure Business Analysts have the necessary level and type of expertise to perform functional responsibilities.

Contractor's approach to ensure that business analysts can perform successfully for the County has four elements:

- Recruiting and Hiring.
- Professional Development.
- Coaching and Feedback.
- Ongoing Experience and Professional Development

Through consistency in Contractor's processes and diversity in its projects, Contractor's business analysts gain growth and experience opportunities they cannot obtain elsewhere. This helps in retention and in the professional development of Contractor's business analysts.

2.22. Chief Technical Architect (CTA)

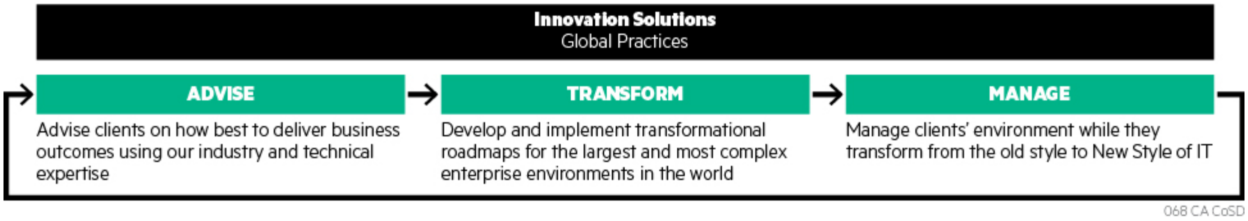
2.22.1. Process and Procedures

- Description of solution to meet the requirements

The Chief Technical Architect (CTA) shall be responsible and accountable to lead the development and delivery of strategic technology solutions that fit the business' needs. The CTA shall work directly with EAA and County Technology Office to review business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services. The CTA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams.

Contractor shall use the methodology illustrated in the figure below, which is based on recognized and proven Open Group practices (HPES RightStep, IT Solution Architecture [ITSA] and The Open Group Architecture Framework [TOGAF]).

Contractor's EA Methodology


Innovation Solutions
Global Practices
ADVISE
Advise clients on how best to deliver business outcomes using our industry and technical expertise
TRANSFORM
Develop and implement transformational roadmaps for the largest and most complex enterprise environments in the world
MANAGE
Manage clients' environment while they transform from the old style to New Style of IT
068 CA CoSD

Contractor's approach enables change and transformation and provides the linkage between key stakeholder groups including business leaders, IT leaders and architects, and Contractor to achieve business transformation.

- Deployment plan for resources and use of facilities

The CTA and the Architects shall be two major components of Contractor's technology team. The CTA shall have overall responsibility for setting Architectural direction and strategy (with CTO), identifying emerging trends, anticipating and understanding transformative shifts in technology, developing enterprise and departmental roadmaps, and maintaining strong relationships with Contractor's leading technology partners. The CTA shall then translate this information and direction to the Architects for execution.

The Architects, who shall receive strategy and direction from the CTA, shall be responsible for executing that strategy including adherence to methodologies, standard processes, best practices, accelerators, and standards.

The CTA shall report to the Account Executive, and the Architects shall report to the Contractor's Technology Office. The structure unencumbers the CTA from the administrative burden required when one has direct reports, including HR activities and staff professional development—these activities shall be the responsibility of the Contractor's Technology Office.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall adhere to proven methodologies and processes across the organization that it adapts to meet the County's requirements.

Contractor shall align with its proven architectural methods (RightStep and ITSA) and holistic focus that encompasses business, data, applications, infrastructure, network, security, management and implementation aspects including solution evolution.

Solution Design Documents

SECTION TITLE	CONTENTS
Executive Summary	<Write a brief introduction describing the focus of this design document including, if applicable, the purpose, background and scope that affect the design of the project. This summary should be written in nontechnical terms as an introduction to the technical sections. It should contain enough information for a reader to get familiarized with what is discussed in the full document.>
Client Opportunity	[Use this section to describe client opportunities, problems, business drivers and/or goals. Include quotes or comments from clients if appropriate. Where appropriate, personalize the document for the client, mentioning the customer name and specific topics related to their environment.]
Proposed Design	<This section describes the logical and physical solution design including the physical architecture. Include one or more diagrams of the design either as an embedded picture or in the appendix. It is important to highlight that this template just provides guidance which must be tailored by the architect or engineer for their specific work. Not all sections and subsections are applicable to all solutions, and there may be some key ones missing for the solution you are designing. This is a template to help jumpstart the work at hand and provide ideas for design content that otherwise might be left out.>
Business Architecture	The business architecture defines the manner in which business strategy/mission, vision, governance, organization and key business processes come together to define the activities that deliver on the business strategy. Business architecture can be developed with a scope that encompasses an enterprise or solution scale. <This section is used if the impact to business from the implementation of this solution needs to be understood by the client stakeholders. For example, if there are significant changes to the way the client does business {business processes, roles of the client employees, business organization, etc.) here you would describe the logical changes to the business architecture. Each section would include the current and proposed architecture.
Data Architecture	< Data architecture provides a blueprint for the structure of the information components in the context of the business processes and the business organization, the application systems and their interactions (integrations), as well as the relationships between them. This includes the data, data service interfaces, and data management components and can be developed with a scope that encompasses an enterprise, solution or technology scale.
Applications Architecture	< Application architecture is the blueprint for the individual application systems to be deployed, their interactions (integration) and their relationships to core business processes of the organization. Application architecture can be developed with a scope that network requirements or touch points.
Infrastructure Architecture	Infrastructure architecture describes the software and hardware that effectively enables the deployment of other architectures. This includes IT infrastructure like servers, storage, backup devices, End-User devices, middleware, processing and standards used in operations, and does not include the network or communication components which have their own section. Infrastructure architecture can be developed with a scope that encompasses an enterprise, solution or technology scale.
Network Architecture	Network architecture describes the software and hardware that effectively enables the connection between infrastructure components and architectures. This includes networks,

SECTION TITLE	CONTENTS
	firewalls, load balancers, WAN, LAN, VLAN, communication devices and appliances, infrastructure device placement within the network, and the associated network standards used in operations. Network architecture can be developed with a scope that encompasses an enterprise, solution, or technology scale.
Security Architecture	< Security architecture is the blueprint for the structure of the security components of the overall solution, and how they are maintained in line with the security policies, both principles and requirements. It provides the central definition of the capability independent threat and vulnerability structure as well as disaster recovery. A security architecture can be developed with a scope that encompasses an enterprise, solution or technology scale.
Acceptance Criteria	<Describe the success criteria and acceptance requirements guidance. This is at high level; acceptance test plans are created later in the lifecycle guided by these criteria but with much greater detail. This is to provide guidance to the architecture and design on how successful outcome is measured by the stakeholders/client. business acceptance criteria would be those measured in terms of business goals, drivers, metrics, outcomes or results, if any ("Improve claim handling productivity by XX%">. Functional acceptance criteria by those that measure what is included (if the many areas of scope were included, functionality of given modules or components, non-functional requirements or qualities). Technical acceptance criteria are related to "how" the solution is put together (how the layers are put together {three tier architecture for example}, how the interfaces work, how the roles are spread across the many environments, etc.). Implementation acceptance criteria revolve around "with what" and in what order the solution is made {for example, database was required to be on Oracle, middleware and ESB using TIBCO, small project implemented first and later phased to full production, support personnel training, documentation standards and content, etc.}.
Implementation Considerations	<Describe the items that were addressed during the design phase of the project for implementation.>
Deployment	<Describe the technical details of the solution's deployment. Include architecture diagrams.>
Infrastructure Management	<Describe how the infrastructure is to be managed, operated and which companies or organizations are responsible.>
Maintenance Plan	<Provide an explanation of the ongoing maintenance support model. Include reference to any existing agreements as well as any new procedures, processes or resource units.>
Evolution	<Describe the evolution requirements or special considerations that affect project planning and solution implementation aspects—order of implementation of the many components, changes in solution scale /size during the various implementation phases, bringing in highly specialized or hard to find resources, etc. This is not a repeat of other sections of the solutions, this is an extract of what project managers should watch for and take into account in the implementation, testing and development planning.>

RightStep and ITSA shall align with the Contractor framework and governance for consulting services, to facilitate integration with all other supporting methods and disciplines—grouped under the umbrella of the Contractor transformation framework. This framework shall align and integrate the architecture with other Contractor capabilities and methods that are necessary for successful transformation including business consulting, value management, management of change, program and project management, portfolio management, IT service management, SOA services, and governance.

Use of Tools

To create architectural designs, Contractor shall use modeling tools such as EA Sparx, ProVision, and/or MEGA to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the Contractor architecture team shall introduce MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

Application Architecture

Contractor’s applications architecture shall include application principles, integration models, application landscape models, application portfolio maps, application to process maps, application flow models, application to information matrix, and application standards, among others. These are organized within topic areas (sometimes called domains and subdomains) and supported by RightStep, as described above.

Staffing and organization of Architecture Services.

Contractor’s global architecture capability is an organization with a formal charter and governance model within ES that supports all aspects of architecture services—methodologies, processes, best practices, accelerators, standards, and professional development. This applies to all architects, whether enterprise, solution, business, or technology architects. This is consistent with Contractor’s approach to create architectures that seamlessly provide guidance from the enterprise scope to the solution and technological layers. The guidance and standards provided by the ES architecture capability team is also used by other business units. Architecture capabilities/teams reside throughout Contractor’s organization, in both accounts and in local and regionally available teams that can be leveraged as an element of a client engagement. To facilitate the organization of architecture services, a collective set of standards, best practices, tools, and accelerators for each strategic capability are kept within the Contractor’s EDGE platform.

Common architecture toolset and documentation standards

Contractor architects shall regularly conduct whiteboard sessions with other team members— security, application, the County, and other vendors—before Contractor creates an SDD for any project. The updated SDD template, included in the Solution Summary and Rationale section above, shall cover all necessary architecture artifacts and design consideration, which shall include high availability, scalability, County architecture/network patterns, reuse of existing County technology assets, leading to complete, consistent and coherent solutions. Contractor shall also use this document for internal reviews as the standard template for architecture projects from start to finish. Every SDD document shall also be used in its entirety in downstream activities, for example, by engineers for technical design documents, run books, server builds, load balance workbooks, and firewall changes. This approach facilitates consistency across all projects from design through implementation.

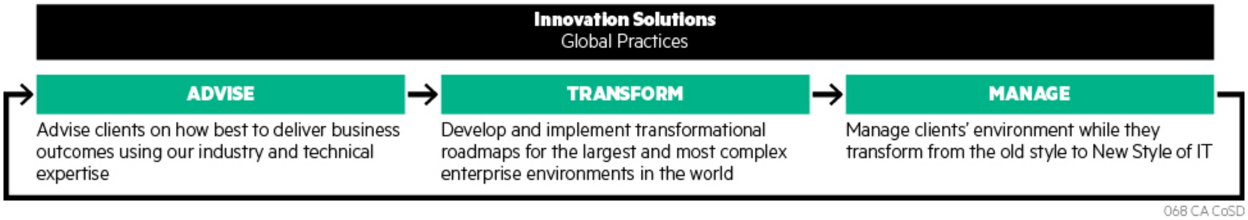
2.23. Enterprise Application Architect (EAA)

2.23.1. Process and Procedures

- Solution Summary & Rationale – Description of solution to meet the requirements

The Enterprise Application Architect (EAA) shall be responsible and accountable for the "advise to manage" (illustrated in the figure below) portion of the enterprise architecture, while supporting the CTA, CISO and County Technology Office in the "strategy to technology" portion. The EAA shall work directly with CTA and County Technology Office to review business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services. The EAA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams. The EAA shall provide the bridge between County business and the IT staff that ensures that the application architecture meets business goals and objectives, that promotes reusability and provides data and interface connectivity across the Enterprise.

CONTRACTOR'S EA Methodology


Innovation Solutions
Global Practices
ADVISE
Advise clients on how best to deliver business outcomes using our industry and technical expertise
TRANSFORM
Develop and implement transformational roadmaps for the largest and most complex enterprise environments in the world
MANAGE
Manage clients' environment while they transform from the old style to New Style of IT
068 CA CoSD

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The CTA and the EAA are two major components of the Contractor's architecture team. The EAA shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements and act as a subject matter expert on the effective use of technology in developing County business solutions. Working with the CTA, County Technology Office and CISO, once overall architectural strategy and direction has been established, the EAA shall advise IT staff regarding the feasibility of their proposed approaches to project solutions in terms of systems capabilities, new technologies and alignment with established application architecture guidelines and standards. The EAA shall have overall responsibility for IT strategy execution across the enterprise including adherence to methodologies, standard processes, reference IT patterns, accelerators, and standards.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall adhere to proven methodologies and processes (RightStep and ITSA) across the organization that are adapted to meet the County's requirements. Contractor's Architecture Services Methodology is based on principles that the County Technology Office has adopted—principles precede requirements and they help frame the overall solution approach to align with County strategic direction.

Processes: Contractor has two primary architecture methods recognized by The Open Group (HPES RightStep and ITSA). Since the EAA is focused on solution development across the lifecycle, the EAA shall primarily use Contractor's Global Method of IT Strategy and Architecture (ITSA). ITSA is Contractor's methodology for developing solution, initiative, or technology architectures. It is a structured as a participatory approach that involves key stakeholders in the client's business. It has been proven effective through many years' experience in defining, guiding, and evolving complex information systems in multiple application domains. ITSA helps architects understand the needs of all stakeholders by viewing the architecture from four vantage points or views:

- Business View – *Why* is the engagement being done? What are the motivations and business drivers?
- Functional View – *What* will the system do? What information will it provide?
- Technical View – *How* will the system be realized with IT components?
- Implementation View – *With what* specific products and other components will the system be implemented? In what organization? According to what plan?

ITSA defines each view using principles, models, and standards appropriate for the business domain. When combined, the four views enable Contractor to understand the needs of all stakeholders and create a snapshot of the solution. Business factors (drivers, goals, metrics, principles, models, and standards) are the basis for all technical and implementation decisions. The methodology does not specify (or limit) the techniques to use to gather the business information or products to solve the customer's problems and compliments each client situation to determine business need, maturity, and existing standards.

- Automated Tools

To create architectural designs, Contractor shall use modeling tools such as EA Sparx, ProVision, and/or MEGA to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the Contractor architecture team shall introduce MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

2.24. Innovation Management Services

2.24.1. Process and Procedures

Innovation Management Services shall support the transformation and innovation model of continuous progressive change in how Services are delivered. This shall include, but is not limited to, delivering Services via a bimodal approach, with an emphasis on exploration, agility, and speed, while still maintaining operational integrity and stability.

Innovation Management Services shall begin at Transition completion with presentation of a qualified Innovation Officer (IO) to the County for County approval. The IO shall develop for County approval a program charter and rules of engagement that define the process to:

- identify potential needs/issues/gaps/opportunities for improvement
- create a list of potential services available to further innovation and transformation, to include:
    - joint development workshops
    - white-board sessions
    - prototypes
    - pilots

    - demonstrations of products, software or services
- design and develop lab environment(s) and rules of use
- determine method to define success criteria
- define collaborative engagement model with EA, CTA, EAA, CISOs and County Business Leaders

Innovation Management Services shall include an Innovation Management Office that shall serve as the foundation for continuous business improvement, innovation, and transformation. The Innovation Office (IO), planned for January of CY2, shall be composed of the Innovation Officer and additional on-demand resources, upon County Approval with the directive to drive IT innovation/transformation and create a true environment of agility and high-velocity change at the County.

The IO shall create and update in the Standards and Procedures Manual the necessary information for the Innovation Management Review Board.IO shall work with County Technology Office and County Business leaders to identify specific actions in support of County Excellence Goals. This results in a series of initiatives in which Contractor shall propose solutions, business case analyses, anticipated pricing, and project timelines and resource plans. The proposed initiatives shall be reviewed by the Innovation Management Review Board and, if approved, shall be executed using (as appropriate) agile and rapid-prototyping methodologies.

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The Innovation Management Office shall be a virtual office with some members residing at CAC and Contractor's Rancho Bernardo facility and others at US-based facilities as determined by skillset required.

Starting after CY1, Contractor shall provide Resource Units rates for the following three (3) resources or more to be used on-demand, upon County approval:

- Senior Technologist (skillset akin to CTA)
- Senior Solution Architect
- Senior Business Analyst

The above resources shall be billed at the Innovation Core Team Member rate as defined in Schedule 16.1 (Fees) – Exhibit 16.1-1 or any applicable labor category rate if it is lower. Any of these labor category rates are to be consumed against the 50%/50% jointly funded Innovation Fund as defined in Schedule 16.8 Fee Adjustments.

Additional personnel ebbs and flows through the Team as required by Innovation/Transformation ideas/pursuits/opportunities.

Additional personnel may come from the County, Contractor, Contractor's partners or other 3rd parties and could include:

- Business Leaders
- Senior Technologists
- Innovation Lab Personnel
- Local Government advisory personnel (e.g.: Gartner)
- Architects/Engineers
- Business Analysts

- Software Specialists
- Logistics Engineers
- Mobility Specialists
- Change agents
- Logistics experts
- Asset and Billing Specialists
- Government Strategists

At execution, Contractor shall propose utilization of an existing RU aligned with the skillset of the team member. If an existing RU cannot be utilized for the activity to be performed, Contractor shall propose an hourly rate or FFP for County consideration. Rates shall be agreed upon in writing by the Parties.

- Processes including year-to-year continuous improvement

Methodologies and key processes shall be defined by the charter and rules of engagement.

Governance shall be provided by the Innovation Management Review Board, co-chaired by County CIO and Contractor AE who shall have joint approval on all proposed initiatives and activities.

Contractor shall perform an annual assessment of Innovation Management Services for County review and approval as part of Schedule 5 reporting requirements.

3. SERVICE DESK SERVICES

3.1.1. Process and Procedures

The Contractor solution to meet the requirements

The following shall be the various support tiers and transfer types used by Contractor:

Support Tiers:

Tier 0 – Self Service
Tier 1 – FCR (anything that can be addressed by the initial agent with no transfer)
Tier 2 –Ticket transferred to a second level agent for support for resolution of an issue requiring on-site support or additional administrative permissions (typically applies to feature functionality issues i.e. Operating System, Browser, MS Office Programs, etc.)
Tier 3 – Ticket transferred to a 3rd level agent (framework) for resolution. Datacenter, Applications, Security, Network, Vendors/3rd party, on-site, engineering, etc. Feature functionality issues typically require specialized support and advanced permissions to resolve the issue
Tier 4 – Global administrator/engineering/architecture required to resolve the issue

Unless otherwise provided in the script documentation the following Transfer Types shall apply:

Transfer Type	Description	Priority
Cold	Ticket sent straight to frame work in the ticketing system with no communication	P4/P5
Warm	Chat E-mail Text	P3/P4/P5
Hot	Phone call	P1/P2/P3

The Contractor Service Desk for the County shall serve as a single point of contact and the primary owner for monitoring and tracking of all incidents and Service Requests (SRs) for approved End-Users. Contractor's key solution strategy is to use ITIL-aligned processes to meet requirements, achieve 70% first-call resolution (FCR), and achieve 12-minute phone handle time as well as Service Desk ownership for end-to-end tracking of all tickets and SRs. Contractor's Service Desk shall use a knowledge documented in the electronic Knowledge Management System (EKMS) to make a swift determination on whether an issue is warm transferred to Contractor's remote desktop/device management (RDM) capability or escalated to deskside/field support or the appropriate framework (e.g., Applications M&O, End User, Network).

Contractor's updated training processes shall provide agents with in-depth knowledge of County processes, scripts practice, and ITIL-based practices. Contractor shall ensure all employees including new hires receive Contractor's Doing Business with the County instruction and monitor individuals for its completion. Contractor integrates the training activities Contractor's agents receive with real day-to-day work assignments. Contractor's training increases agent comprehension of County-specific issues and expertise in routing tickets efficiently and effectively to the appropriate technical support group. shall identify those agents who require additional instruction and customize training to strengthen their skills.

As Contractor implements the self-service technologies of the Agreement, Contractor shall encourage users to access the Service Portal's self-service functionality from their desktops, tablets, or mobile phones. Contractor shall provide its technology End-User adoption approach,

Contractor's HPSM system's data analytics functionality shall include documentation and display on the Service Portal of Service Desk statistics tied to both Contractor's team's objectives and the County's service levels. The data warehouse, accessible through the Service Portal, shall contain County attributes for reporting and analytics such as PA-ID, POETA, County Group, and County Department. Contractor's Service Desk manager shall perform quality reviews on relevant areas such as call waiting/call abandonment, efficiency in meeting the phone time to resolve metric, rate of FCR success, and End-User satisfaction levels upon ticket resolution. On systematic review of trends, surveys, and reports, the Service Desk manager, together with other members of the Contractor account management team, shall find opportunities for improvement of Service Desk services and operational cost efficiencies.

Service Desk Structure

Service Desk.

Contractor agents shall be the first point of contact and if needed shall provide remote desktop/device management (RDM). If support requests cannot be resolved by the first contact agent (Level 1), then the call shall be escalated to RDM (Level 2). In some cases, the Service Desk agent escalates to the deskside/field team or subject matter technical support (Level 3), which includes frameworks such as applications, engineering, exchange, data center, infrastructure, storage, etc. Level 1 and Level 2 resources shall reside within the Service Desk Framework. Level 3 support shall be provided primarily by the various frameworks unless the Service Desk has the ability to resolve the issue based on the documentation provided by the framework and has the required access to the systems. Contractor shall provide to all agents Service Desk training and detailed documentation outlining the correct escalation path for each type of incident or SR that guides agents to make certain that tickets requiring escalation are routed correctly the first time.

While the Service Desk Framework is responsible for the full life cycle and management of all incidents, installs, moves, additions, and removals (IMARs), and SRs, each framework shall be responsible for management of its work stream, making certain that work is triaged within the required timeframes. Points of contact (POCs) are identified within each group to manage these activities and verify work is completed. Costs associated with these activities outside of the Service Desk agents shall not result in additional costs to the County.

Remote Desktop Management (RDM). Service Desk agents shall use RDM to interact with network services, software systems engineering, and/or an applications group to restore service and/or identify and correct problems. This may require assisting in simulation and recreation of End-User problems and recommending systems modifications to reduce End-User problems. Service Desk agents shall be facilitators between customers and other support teams to make certain customer needs are met and tickets are resolved in an expeditious manner.

Comprehensive Service Desk for the County

Contractor shall continually add to the knowledgebase, working closely with other resolver groups to identify areas where Contractor can improve knowledge documentation to provide increased resolution at first call, freeing resources to support their other activities.

Deployment plan for resources and use of facilities

Resource Management — Oversight for Service Improvement. The Service Desk manager shall provide oversight of performance, resource management, and service delivery, including the collection, consolidation, and dispatch of events and information sent by the County as it relates to the environment. As part of this role, the

Service Desk manager shall review metrics on customer satisfaction and success in meeting County requirements and establish quality processes and intensified training approaches to improve Service Desk performance. Contractor's reporting analyst shall analyze Service Desk data, identifying and adjusting metrics queries, and fulfilling the ad hoc Service Desk-related report requests from the County and from the Contractor service delivery manager in the County.

The Service Desk manager shall lead daily status calls with the Service Desk Workflow Manager (Workflow Manager), operations manager, and shift leads to make announcements, communicate County concerns, and review the status of any issues that emerged overnight. In addition to the daily status calls, the Service Desk manager shall call meetings every Monday before each shift begins that include the agents on deck. These meetings shall provide a venue for management and agents alike to raise issues they need to address and to foster interaction with the Service Desk manager in his efforts to support alignment with County expectations. Contractor's Service Desk support shall concentrate agent numbers in shifts during the County's core hours from 6:00 a.m. to 6:00 p.m. PT, Monday through Friday, and maintains support overnight and weekends.

The Workflow Manager shall support the Service Desk manager in providing day-to-day supervision of operations, monitoring that agents arrive on time and are attentive to their responsibilities, adjudicating rotation of shift personnel, and making sure that the metrics gathered on Service Desk are uploaded properly on the Service Portal for review by the Service Desk manager, the quality analyst, the Contractor account team, and County administrators. The workflow manager shall constantly communicate with the Service Desk manager, updating him on Service Desk issues throughout the day, workloads, and staffing, including issues of individual agent performance.

Working with the Service Desk operations manager and scheduler, the shift leads shall monitor the ticket queue to make sure tickets do not go unattended. Other shift lead responsibilities include providing oversight of ticket agents' handling of Priority 1 and 2 Incidents and High Response End-User/Critical User tickets. Contractor's shift leads shall oversee agent performance and work with the Service Desk's training analyst to develop measures to improve expeditious handling of tickets and effective agent–End-User interaction. Contractor's training analyst shall check the training history of individual staff, making certain that all staff take Contractor's mandatory training, and shall provide follow-up as necessary.

Key methodologies and processes including year-to-year continuous improvement

IT Service Management (ITSM) Processes for Service Desk. Contractor shall implement ITIL/ITSM processes for Service Desk with a focus on customer service satisfaction and continuous improvement. As a key ITSM framework process, Contractor's Service Desk shall own and track tickets created at initial call or that are assigned via the Service Portal, and it is their responsibility to maintain open communication channels with the End-User in the event of a ticket inquiry throughout the ticket's life cycle. Contractor's Service Desk agents shall also provide an interface for activities such as SRs, customer change requests, incident management, and third-party support.

Continuous Improvement. ITSM shall collect data from the Service Desk system, Customer interactions, HPSM, the Avaya CMS Call Manager, and the Customer feedback surveys that Contractor uploads for data aggregation and review. All of the data input from these systems along with the additional reporting that Contractor adds from chat and Self Service shall be placed into the analytics environment that is created in support of the Service Portal. Service Desk related data shall be posted to the Service Portal and reviewed regularly with the CTO during the Operations status calls.

Quality Monitoring to Improve Agent Overall Performance and Customer Service. Contractor's Service Desk manager together with the workplace manager and shift leads shall review the results of the customer satisfaction surveys and other relevant data displayed on the portal (for example, phone handle times at initial call, ticketing information, chat data, most common scripts used, etc.) to discover areas for improvement, discuss them with the quality assurance (QA) analyst for Service Desk, and present findings at a Monday all-hands Service Desk meetings for each shift.

At these meetings, managers and leads shall make recommendations on issues identified or for the agents to raise new problem areas they have experienced the previous week. The workplace manager shall upload results and new resolutions from the meeting to the Service Desk dashboard reserved for agent posts. As each shift conducts its Monday meeting, additional comments shall be added to the dashboard. These recommendations shall be communicated by the Service Desk Manager to the CTO.

Contractor shall implement the following five-step quality management framework, supported and documented by Contractor's QA analyst: (1) Monitor Performance; (2) Analyze Performance; (3) Identify Areas for Improvement; (4) Establish Corrective Actions; and (5) Verify Improvement. The framework aligns with Contractor's seven-step ITIL processes for continuous service improvement.

Monitoring Performance of Individual Agents. Contractor shall capture agents' voice interactions with users along with the corresponding computer desktop activities, such as data entry for logging tickets, cataloging and prioritization, screen navigation, and data retrieval from the knowledgebase. To effectively coach employees, Contractor shall use two quality monitoring methods: side-by-side and remote. In side-by-side monitoring, the shift lead shall use a headset to join the call of a new agent or an agent learning better communication skills. The shift lead shall also use remote monitoring—that is, agents are unaware they are being monitored—to audit and evaluate agents' performance for Contractor's quality metrics.

Contractor's Service Desk manager shall consult with the workplace manager and shift lead to perform agent evaluation review and identify patterns to assist agents in understanding how each aspect of their performance affects the whole.

Automated systems and tools involved in Contractor solution

Contractor shall implement for the County HPE Service Manager (HPSM), Contractor's system that includes comprehensive core and extended Service Desk advanced functionality. It shall provide key Service Desk automated processes and manage Contractor's responses to County users, including first call resolution (FCR), deskside support coordination, and ticket and SR escalation to support, including to AT&T network/mobile SMEs and other vendor support.

Contractor shall implement the Service Portal and its self-service capabilities within 90 days of the Contract Effective Date. The portal implementation approach as detailed in the Transition section for the Service Desk shall include the core functionality of new services and links to current data sources and source systems to integrate with current repositories within the 90-day timeframe.

At the end of the transition period End-Users shall be able to perform the following via self-service:

- online -ticket creation
- Review status of tickets and Service Requests,
- Perform online password resets via the Self Service Password Reset, SSPR tool
- Conduct chat sessions with the Service Desk for information or support
- View reporting.
- Access to the Knowledgebase (FAQs, tips sheets
- View Outage Status, Trending Now, and Announcements

- Access to MyRequests, and various links (ITSC, DocVault, etc.).

The new service catalog that replaces myRequests and the complete integration of the configuration management systems (Asset Manager, Apps Manager, ESL) shall be implemented as a part of the transition and is included under the Cross functional transition section and timeframes. Contractor shall engage the CTO and other relevant County stakeholders to provide input into the look and feel of the portal. County users shall be able to access the Service Portal, including self-service functionality, from their desktops and other platforms.

On-Going Maintenance, Support, and Enhancements: The Service Desk Manager shall be the primary point of contact for the Service Portal for the County of San Diego. Technical support and enhancements shall come from the Contractor's Portal framework, which is a leveraged team. The Service Desk Manager shall make certain that issues related to the portal are being resolved and that maintenance items and new features are being implemented as needed.

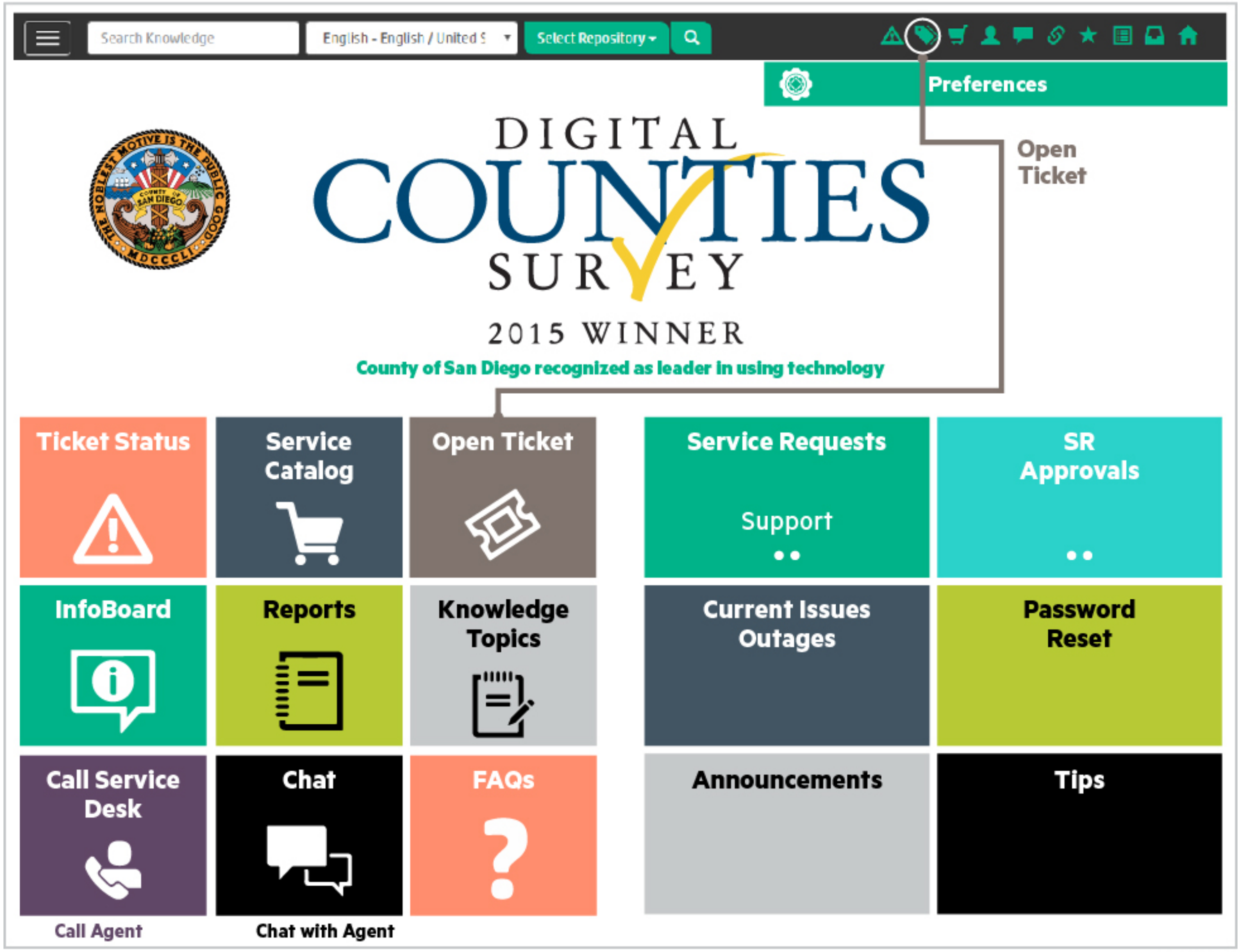
Contractor shall follow a quarterly maintenance schedule for changes to the portal that are non-incident related and for changes that may require coordination, training, and communication to the End-Users. Simple changes (adding links, contacts, FAQs, Announcements, Trending Now information, etc.) shall take place on a frequency agreed with the County. The overall focus around the processes and frequency related to these changes shall be to ensure the latest and most accurate information is published to the portal in a timely fashion to benefit the End-Users. Once the timelines are established, processes shall be built, approved and communicated as required. To make certain that the changes being made are communicated, well thought out, and in the best interest of the End-Users, the Service Desk Manager shall be a part of a Portal Review Board, the final composition of which shall be established by the CIO, in consultation with Contractor Account Executive, to discuss, approve, document, and communicate all changes related to the Service Portal. These changes shall include not only the content within the Service Portal but the processes related modifications that need to be made over time to ensure information and Service Portal accuracy. For changes to the Service Portal that require Portfolio Application modifications or County data manipulation, a Budgetary Estimate (BE) shall be provided to the County to determine how or whether to proceed with these changes.

Training: Training shall be provided for all End-Users and support staff as a part of the Transition project related to the Service Portal. This shall cover every aspect of what is in place at the end of this project. As a part of transition planning, Contractor shall discuss with the County the various training options and communications that are needed to ensure that all End-Users understand the capabilities of the portal and how the portal works.

Sample Landing Page for Service Portal with Self-Service Functionality

Unless otherwise agreed to by the County, the landing page for the Service Portal shall be substantially similar to the following:

Portal – Landing Page



060 CA CoSD

County users shall be able to click a tile to phone Service Desk, open a ticket on their own, reset their own passwords, make SRs, check County announcements, access training, FAQs, and Tips, and stay alert to outages. In another example, upon clicking "Open Ticket," a dropdown menu appears that allows the End-User to select from a list of problem categories; once the category is selected, a second dropdown menu appears with category-relevant problem descriptions. During the process, if the End-User decides guidance is needed from a live agent, he or she can click the "Chat" tile or "Call Service Desk" for support.

When a ticket is created from the portal or the Service Desk via a phone call or email, Service Desk shall embed the End-User's profile (i.e., contact information, location, and asset information) in the ticket and track it until resolution, posting updates on the ticket's progress on the portal. The solution shall allow the End-User to easily obtain ticket status by accessing the portal landing page from his or her desktop, tablet, or mobile phone.

The fully-implemented HPSM shall include myRequests.

Ownership and end-to-end tracking of Incidents

Service Desk shall have ownership of all tickets and shall track them from End-User submission through ticket resolution. Contractor shall use ITIL-aligned processes. The Service Desk agent shall update the End-User on ticket progress until it is resolved.

Service Desk Handle Time and Escalation of Incident Tickets. When an End-User calls in an Incident by phone, the Service Desk agent who answers the call shall own the ticket. The agent shall first verify whether the call is for an Incident rather than a SR. Once an Incident is validated, the agent shall log the ticket, including the End-User profile, categorize the Incident, and prioritize the ticket according to the County’s priority matrix (i.e., Priority 1–3); if the caller is on the High Response End-User list, the End-User profile shall automatically alert the agent to register the ticket as Priority 1 or 2 depending on the severity of the issue.

If the Incident arrives through an End-User-created ticket via the Service Portal, its automated processes shall upload it to the ticket queue for selection by available ticket agents. Ticket assignment order shall be determined by first in/first out and by severity. Severity 1 and Severity 2 tickets shall receive immediate attention by Service Desk agents, with oversight by the Workflow Manager and Shift Lead.

Once the Incident is logged, the Service Desk agent shall assign the ticket, start troubleshooting, and diagnose it using information provided by the caller or the description on the portal-generated ticket. The Service Desk agent shall quickly resolve low-level Incidents associated with known errors by applying approved solutions or workarounds. In cases where the Service Desk agent may know immediately that the Incident cannot be resolved, the Service Desk agent shall determine, based on knowledge documented in the EKMS, whether it can be routed to deskside/field support or to the appropriate framework for resolution. In some cases, vendor-specific support may be required. The knowledge incorporated in the EKMS shall derive from information provided by the vendor on its hardware/software; resolution and workaround instructions developed by Contractor’s SMEs based on their respective areas of expertise (e.g., applications, network); and information developed by the County SMEs on its infrastructure.

Deskside Support Escalation. When Contractor’s deskside technicians receive a ticket, they shall retrieve all the service attributes from the EKMS and launch scripts and perform progressive troubleshooting based on the documented knowledge to identify the probable source of a service Incident. For example, if Service Desk performs troubleshooting and is unable to resolve the ticket, the Service Desk agent shall itemize the actions taken and issues still unresolved on the ticket’s Comments section. Service Desk shall notify the End-User that the ticket needs further troubleshooting deskside; the technician shall coordinate the date and time for the visit with the End-User and post the appointment in the ticket. The ticket information, including scheduled deskside visit, shall be viewable via the Service Portal.

Subject Matter Expert (SME) Escalation. When the Service Desk agent recognizes that the source of the Incident requires SME support, he/she shall escalate the ticket to the SME support team appropriate to the affected framework.

In addition, Service Desk shall escalate unresolved “child” tickets that match a “parent” ticket to the SME support team working on that Incident’s resolution. The SME support teams shall perform additional diagnostics, as necessary, to identify and implement an appropriate solution or workaround. These teams shall take a comprehensive approach to resolution, keeping in mind the parent/child ticket linkage and recording their actions in the Comments section of the ticket accordingly. Once the issue is resolved, the Service Desk shall update the status of all the linked tickets on the Service Portal and notify all impacted users.

Vendor Support Escalation. When a ticket is escalated to a Third Party regarding a product that cannot be resolved by Contractor’s deskside technicians, the Service Desk ticket owner shall confirm that the problem is fully described on the ticket before it goes to the vendor’s helpdesk.

Ticket Closure. Once the ticket is resolved, the resource responsible for the resolution shall change the status of the ticket to “Resolved.” This action shall automatically notify the End-User via email of the resolution. The body of the email shall request a reply within 3 days if the issue was not resolved to the End-User’s satisfaction. If no answer is received after 3 days, the ticket status shall remain “Resolved” for an additional 7 days in case the End-User is out of the office. If the End-User does not reply after the additional 7 days, the ticket shall automatically be set to "Closed." Contractor shall continue using this format to update the End-User on resolution if desired by the County, but at the County's option, Contractor shall implement a verification email that shows the End-User how the ticket was resolved, encourages the End-User to complete the customer feedback survey, and promotes the County's self-service password reset requirement. When the End-User clicks on the respective blue icons in this message, he/she goes to the Service Desk site related to the text.

Maintenance and refresh of Service Desk scripts.

Contractor shall use structured formats for receiving calls and scripts that have proven successful in addressing problems and accelerating resolutions within 12 minutes on Service Desk. Contractor shall develop scripts for RDM and higher-level technical solutions. When the County users request a new script or a modification of a current script, the appropriate technical support group shall communicate with them in developing the script in adherence with Service Desk Script Revision Process documented in the Standards and Procedures Manual.

Contractor's knowledge content analyst for Service Desk shall review scripts for consistency with the database methodology and style guide, recognizing that certain Service Desk scripts are spoken to the caller. Contractor shall maintain successful scripts in a Service Desk EKMS with rules-based access to Contractor's agents/technicians. Contractor shall refresh the information in EKMS and the Self-Service Knowledgebase information annually.

Contractor's Service Desk Manager shall adhere to the Framework Revision Process flow established by the County and post in the Service Portal Contractor's Monthly Revised Scripts—Revision/Acceptance Report, which enumerates the total scripts in the EKMS and the number of revisions that month.

Using HPSM, Contractor shall collect metrics on response and resolution times associated with respective scripts that Contractor's agents use against identified problems.

In reviewing metrics and issues raised by Contractor's agents, the Service Desk Manager shall identify less helpful scripts and assign them for rework. Contractor's development of new scripts or revisions of existing ones shall draw from the HP Global Service Desk scripts, a database of proven scripts to address a range of problems that have demonstrated success on Contractor's accounts worldwide.

Contractor's Service Desk shall support the Service Portal by reviewing the scripts in the EKMS and selecting those appropriate for revision for "how to" instructions with visual aids for upload into the Self-Service Knowledgebase. Contractor shall work with relevant SMEs in developing suitable language for End-Users accessing the Service Portal's self-help functionality. This shall include tips, training and FAQs.

Preventing abandoned calls

Contractor shall increase Contractor's training of Service Desk agents, both new hires and incumbents, to increase their ability to resolve tickets quickly. This training shall include Contractor's indexed Knowledgebase and scripts to resolve less complex Incidents quickly at first call. For callers making SRs, the trained Service Desk agent shall point the caller to the related content in the Service Catalog for products and direct the caller on how to use the SR tool on the Service Portal.

Additional Measures: Contractor shall take measures that shorten the phone handle time to restore service to the End-User as quickly as possible and allow the agent to help the next End-User.

- Contractor shall provide Contractor's agents with a Self-Service Knowledgebase with an indexed search engine at their fingertips;
- Contractor's agents shall open their response to the caller with a time-saving structured format (template)
- The call waiting recording shall provide the option for the End-User to leave voicemail to be returned within 15 minutes

First call resolution strategy

Upon receiving a call, the Service Desk agent shall access the Service Desk module's dropdown menu, which shall provide a range of predefined problems or SRs.

A Service Desk agent shall quickly assess the issue and determine if it can be resolved by the agent or must be escalated for SME support.

- Contractor shall identify data in HPSM to determine overall FCR performance, by contact type and agent identification.
- Contractor shall calculate the number of repeat calls on the same issue to identify trends and problems and develop Knowledgebase and "how to" articles accordingly, including tips and FAQs.
- Contractor shall identify Service Desk agents needing additional training.

Resolution of Impacts to County and non-County End-Users

The Service Desk shall quickly identify High Response End-User and critical systems issues, and shall page Contractor's appropriate on-site technical support.

Contractor's HPE Service Desk agents shall provide elevated support when it comes to critical events in the County. Critical or special events include but are not limited to the following classifications:

- County-wide disasters/emergencies. For these events (e.g., fires, floods, power outages), the Office of Emergency Services (OES) is activated and support personnel are required to work with the County to support the End-Users and the public. The size of these events vary, and Local Assistance Centers (LACs) may be required
- Disasters/emergencies that are small in scope. Response to these events (e.g., focused areas of flooding, building damage) are typically initiated by the Business Group that is impacted. In some cases, a relocation is required to continue to provide service, or an LAC must be stood up.
- Elevated service levels are activated for the Registrar of Voters in support of elections.
- Elevated service levels are activated for Treasurer Tax Collector in support of several public-facing activities conducted by the County.

Each of these events shall have a documented process in place to ensure that Contractor's agents and staff not only understand these requirements but also can route calls appropriately for resolution. The Service Desk agents shall have everything they need and be trained to support this effort and are able to distinguish between an emergency event and standard call.

Contractor shall update the High Response End-User priority matrix and a list of County and non-County High Response End-Users as provided by the CTO.

Calls, emails, or Service Portal notifications from these High Response End-Users and organizations shall be automatically flagged at the Service Desk for escalated response. The Service Desk agent receiving the notification shall follow the mission-critical workflow and the Workflow Manager shall provide oversight to make sure the call is escalated if it cannot be resolved right away.

On-site support to End-Users

The Service Desk agent may determine that deskside support is the necessary next step to resolve the ticket. Before escalation, the Service Desk agent shall review the ticket to make sure that all actions taken in diagnosing and troubleshooting have been recorded in the Comments section.

The Service Desk agent shall notify the End-User that the ticket requires a deskside visit for additional troubleshooting. Then the deskside technician shall coordinate, via Chat or on the mobile phone or email, the visit date and time with the End-User. The scheduled time, date, and location shall be updated in the ticket, which shall be available for lookup on the Service Portal.

Once the deskside technician resolves the issue, the ticket shall be set to "Resolved" and shall follow the "Ticket Closure" process described above.

Contractor shall locate Contractor's deskside support personnel at the Rancho Bernardo facility and at the CAC and COC. Contractor shall station Contractor's mobile phone personnel at the AT&T facility on Trade Street.

End-User self-service capabilities

Contractor's self-service solution shall provide End-Users the option of accessing the Service Desk to open a ticket, obtain ticket status, make an SR, check outages, and perform password reset via the Service Portal from multiple platforms, such as mobile phone, desktop, tablet, or Chat.

Chat. As part of the Service Desk transformation, Contractor shall enable users to use Chat with Service Desk agents to request information, report an incident, or request information on SRs. As with other methods of contacting the Service Desk, Chat shall begin with the standardized ticket workflow and ends with successful resolution. Agents can handle multiple, simultaneous text Chats. The chat tool shall come as a part of the HPSM toolset that is being implemented for the County. The End-User shall be able to access this chat functionality through the Service Portal so no additional software is required on the End-User's devices. **Self Service for Incidents/Problems**. The new self-service ticket capability option shall enable an End-User to open a non-critical ticket that is automatically submitted to the Service Desk queue for review and action. The End-User clicks on "Open Ticket" to submit hardware, software, connectivity, printing, phone, and voice issues, as well as general questions. Users shall be able to track their ticket status without contacting an agent by clicking the "Ticket Status" tile on the portal.

Self Service for Password Reset. As a part of self-service, Contractor shall implement HPE's Self-Service Password Reset Tool (SSPR tool). The SSPR tool delivers multiple ways for End-Users to reset their own passwords. This solution removes the requirement for Service Desk intervention where End-Users have forgotten their passwords and/or locked their account. SSPR is a web browser-based, automated password reset tool that uses dedicated infrastructure, within the County's domain. It also provides a Web-Services based API that allows password resets directly from the Logon Screen. SSPR can also be accessed by visiting the SSPR Web Page from any supported browser on any device, provided it is connected to the County's network. Integration with Active Directory shall be completed as a part of Transition. Other repositories to be added as requested by the County via Service Request.

Additional Self-Service Features. Contractor's portal capabilities shall include more features for both self-service and agent assistance:

- Knowledgebase search engine capability that provides users on their desktop, laptop, or phone "how to" instructions for resolving common problems. Contractor's Knowledgebase content shall use standard text information that delivers clear "show me" instructions that walk the End-User through resolution, click-by-click. It shall also provide videos for step-by-step problem resolution.
- FAQs based on Contractor's review of questions typically asked by users and Tips that enable quick search on a range of information.
- Self-service password reset online tool that allows users to securely reset their own passwords without agent intervention. Users access the secure system by a simple web-based interface, such as a County public-facing website, linked to the portal but implemented separately.
- Dashboard view of the end-to-end County IT environment. Both County management and users are also able to view Rich Site Summary (RSS) feeds, system-wide notifications, alerts, and other important information that impacts the overall IT environment.

- Mobile device “click to call” brings easy dialing options to contact a service

Contractor’s approach to introducing the new technologies promotes early County administration and End-User adoption because self-service saves time and improves End-User productivity. Among Contractor’s techniques, Contractor shall host training sessions for County users to demonstrate portal and self-service capabilities. On deskside visits, Contractor’s technicians shall demonstrate functionality and answer questions. Contractor shall distribute tent cards with “how to” instructions on County desks.

End-User survey process

Contractor shall provide a customer survey for break/fix tickets. The format of the survey shall be designed to make it easy for End-Users to assess in as little as a few seconds the level of their satisfaction with the Service Desk and provide comments if desired. Contractor shall consult with the County on the final design of this survey; upon agreement, Contractor shall distribute the survey after ticket resolution via email or mobile phone. The customer survey shall be an automated process. The automated dispatch and collection of the survey shall be independent of Service Desk.

Contractor shall provide survey results on the Service Portal each month for the appropriate CTO staff. The survey shall identify the ticket agent and the type of issue that was resolved. HPSM metrics shall provide the time taken to resolve the issue and the tier level of resolution, including whether Contractor is meeting Contractor’s 70% first call resolution rate.

Contractor’s Service Desk Manager shall collect and regularly review the survey data collected; a reporting analyst shall identify trends and mentoring and training opportunities.

Continuous measurement of Service Desk performance

The Service Desk ticket system, phone reports, and customer interactions and surveys shall provide the data needed to the Service Portal. These data points shall provide the detail that not only makes certain that Contractor is meeting Contractor’s service levels, but provides the level of information that Contractor requires to continuously improve Contractor’s services.

The HPSM Service Desk module shall enable Contractor to standardize the collection of data, collect more categories of data, and provide more accurate data on which Contractor can identify areas that need or demonstrate improvement. For example, dropdown menus with predefined service issues shall allow Contractor to enumerate a standardized selection of issues and determine their average time to resolution. It shall also indicate agents who take longer than the average who may need more training, are working an issue that may require more documentation, or have come across something new that Contractor needs to put in place. Contractor shall follow ITSM processes in tying data collection and metrics to continuous service improvement.

The Service Desk Manager shall define the metrics needed to improve Service Desk customer satisfaction and shall use the HPSM Service Desk’s data collection capability. HPSM logic shall be aligned with ITSM processes, thus allowing Contractor to collect data not only directly tied to the service levels but also more detailed data that support Contractor’s strategy for continuous improvement.

Inputs to this step shall include collecting data against the service levels. HPSM shall have the capability to collect data automatically, including:

- Baseline data on call waiting times
- Call abandonment rates
- Initial call handle time
- Resolution time in Service Desk by agent
  - Categorization of predefined issues and their resolution time

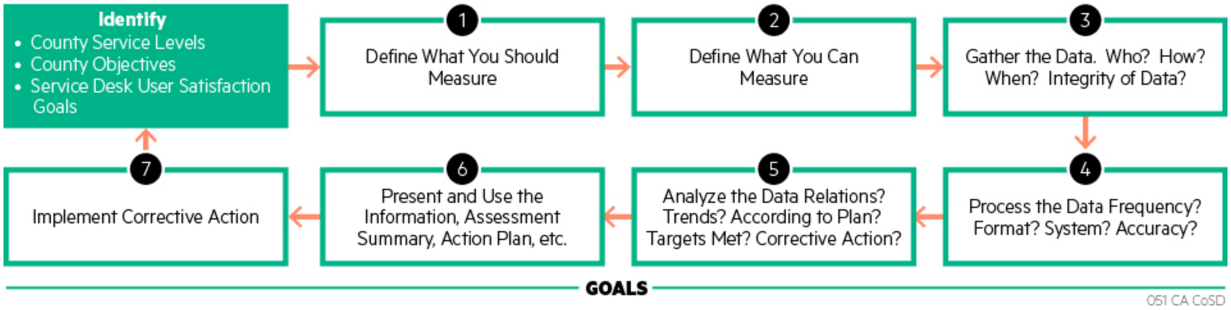
- Customer Satisfaction Survey ratings and End-User comments

Service Desk Manager and Workflow Manager shall conduct a daily operations status call to review and report metrics and discuss issues that may have emerged overnight or are trending. This call shall take place before County standard business hours to ensure Contractor can resolve issues that were raised from the night before. Together they shall review data collected on Contractor's response and resolution times. They shall develop corrective action plans and implementation schedules to improve areas that are lacking or areas where new items need to be put in place.

HPSM has more than 150 reports that Contractor can use to gather information. The reporting and data that Contractor uses from this system can be filtered in any way necessary to for Contractor to either provide the information to those requesting it or to isolate the area in which Contractor need to improve or is making an improvement. Information from the various reports that are needed to support the business shall be provided to the County via the Service Portal and the various meetings that take place (CTO Operations Meeting, Portfolio Review Meetings, etc.). Contractor shall seek direction from the County on the reports to be displayed and who needs to view which set of reports as Contractor moves through Transition and build out of the Service Portal.

Contractor's ITSM-aligned, seven-step process, depicted below, provides a solid foundation for capture and reporting of data to support analysis that Contractor can use to identify opportunities for continuous improvement.

Seven-Step Process for Measuring Performance to Support Continuous Improvement


Identify
• County Service Levels
• County Objectives
• Service Desk User Satisfaction Goals
1
Define What You Should Measure
2
Define What You Can Measure
3
Gather the Data. Who? How? When? Integrity of Data?
4
Process the Data Frequency? Format? System? Accuracy?
5
Analyze the Data Relations? Trends? According to Plan? Targets Met? Corrective Action?
6
Present and Use the Information, Assessment Summary, Action Plan, etc.
7
Implement Corrective Action
GOALS
051 CA CoSD

Error! Reference source not found. describes relevant Continuous Service Improvement (CSI) activities, such as service level reporting and management processes, that Contractor has tied to the Seven-Step Process:

Continuous Service Improvement Service Desk Approach for the County.

CSI ACTIVITIES	CONTRACTOR CSI APPROACH TO SERVICE DESK
Steps 1, 2, 3, 4 Performance Metrics	Contractor shall capture a performance metrics and capture the same metrics every month thereafter for comparison. Contractor shall display Contractor's metrics on the Service Portal metrics dashboard in a meaningful, easy-to-use format for access by Contractor's agents and the County. These metrics shall come from HPSM and the Avaya Call Manager system.
Step 3 Customer Satisfaction Surveys and Assessment	In combination with the performance metrics that Contractor shall use in steps 1 to 4, Contractor shall leverage HPSM Service Desk to collect customer feedback using customer satisfaction surveys. Contractor shall regularly review customer satisfaction surveys and follow up on any negative surveys. This allows a feedback loop into the process for improvement as well as follow-up communication to the customer.

CSI ACTIVITIES	CONTRACTOR CSI APPROACH TO SERVICE DESK
Step 5 Identifying Opportunities for Improvement	Contractor's Service Desk Manager, working with Contractor's Work Shift Manager and agent leads, shall use a real-time portal view of Contractor's Service Desk performance metrics (e.g., call waiting time, call abandonment, Service Desk time to resolution, volume of tickets escalated to different resolver groups), data analysis, and lessons learned to identify improvement opportunities for Contractor's Service Desk team of agents.
Step 6 Daily Agent Meetings Dedicated to Service Improvement	The Service Desk Manager, Work Shift Manager, and Service Desk agents shall meet daily to review areas that need improvement and brainstorm ways to improve performance. For example, if metrics show that Service Desk phone handle time has increased with the use of the script for break/fix, Contractor shall work together to see what phraseology is causing the problem and correct it.
Step 7 Corrective Action Development and Implementation	For serious quality issues, Contractor shall develop a Corrective Action Plan (CAP) with support from the accounts QA personnel that includes a timeline for implementation. Following implementation, Contractor shall gather metrics specific to the issue to measure progress.

Design for the Service Portal

Contractor shall use HPE Service Manager (HPSM) software at the core of Contractor's ITSM Service Desk. HPSM shall include Contractor's integrated Service Portal solution for providing a closed-loop incident process and End-User self-service Incident resolution, SR creation, and information search. HPSM together with the Service Portal shall provide multiple dashboards easily accessible by County users and Contractor management, and Service Desk agents.

Key components of the Service Portal Contractor shall include:

- Access from both the Internet and the County Intranet
- Support for key processes, including incident, problem, change, SR (interaction), self-service, and service asset and configuration management
- Single sign on (SSO) integration and predefined roles and rules
- Improved, standardized screen layout with "smart indicators" to flag related information
- Rich cross-process functionality via a range of wizards
- Management reports, service-level reports, all required County deliverables
- Service Desk-specific components include:
  - Service levels built in with data analytic capability that generates reports such as ticket volume and response times
  - Self-service access to the Service Desk to open a ticket, access the Service Catalog, make an SR (through the SR management tool), access ticket and SR status, see announcements including number of outages
  - FAQs, tips, training, and self-service password reset capability
  - County-dedicated EKMS for technical support teams that includes documentation and flowcharts for processes, procedures, root cause analyses (RCAs), and high-level work around instructions across the frameworks

3.5. Service Request Management Services

3.5.1. Process and Procedures

A self-service indexed Knowledgebase developed specifically for access by all End-Users, upon County approval, to help them obtain the best answers in real time to their request for information and resolve low-complexity problems.

Contractor shall provide Service Desk agent assistance for fulfilling Service Requests (SRs) and to enable users to create their own SRs on the electronic processes of the Service Portal's self-service capability. Contractor's Service Portal shall use HPSM and myRequests, the current application for SRs and ticketing. The Service Portal shall also provide the entry point for other tools such as SharePoint. As part of the Cross Functional Transition phase, Contractor shall migrate myRequests to HPSM's more advanced SR functionality.

Contractor shall work with County to capture and document all SR-related content and maintain it in a rules-based database within the SR Management tool. Contractor shall also develop a Service Portal version of the OIC Service Catalog.

Service Desk Agent SR Assistance. Contractor's Service Desk agents shall assist users with submitting SRs for items such as installs, moves, additions, and removals (IMAR) or changes to the workplace environment.

Service Desk shall provide this service by creating records on SR forms, copying an existing record, or applying a predefined template that prefills specific fields using electronic processes:

- The End-User makes the SR to the Service Desk by phone, email, fax, or the Service Portal.
- The Service Desk agent determines if the SR is a request or an Incident and follows a closed loop process
  - If the request is an Incident, it is handled as discussed in the Incident Management Section.
  - If the request is an IMAR, the agent shall refer to the appropriate documentation to make certain that the request is routed properly to the appropriate framework. Details of this process are provided in the End User Services Section.
- The Service Desk agent categorizes the request and assigns a priority level.
- The Service Desk checks the Service Catalog, which is based on the OIC Service Catalog, to determine if the SR needs approval and, if so, the level of approval required.
- If a request is approved, the Service Desk agent escalates it as appropriate, and updates the End-User upon request.

Service Portal Service Catalog. Contractor shall develop a version of the OIC Service Catalog suitable for Service Portal self-service. The portal's version of the Service Catalog shall be accessible to all End-Users for making Service Catalog-based SRs. The SRs shall display the approval process required to the End-User before being routed to the Service Desk. A Service Portal version of the Service Catalog shall provide the following benefits:

- Reduces Service Desk's workload by providing self-service capabilities for Service Catalog requests that flag approvals that are required
- Ensures all self-service SRs are routed to Service Desk for review
- Provides a single, guided, questionnaire-style End-User interface for requesting support for catalog and non-catalog items
- Provides tablet and mobile End-User support.

4. End-User Services

4.1.1. Process and Procedures

Assessing and mitigating impacts to existing desktop systems and business applications while transitioning to new standard platforms.

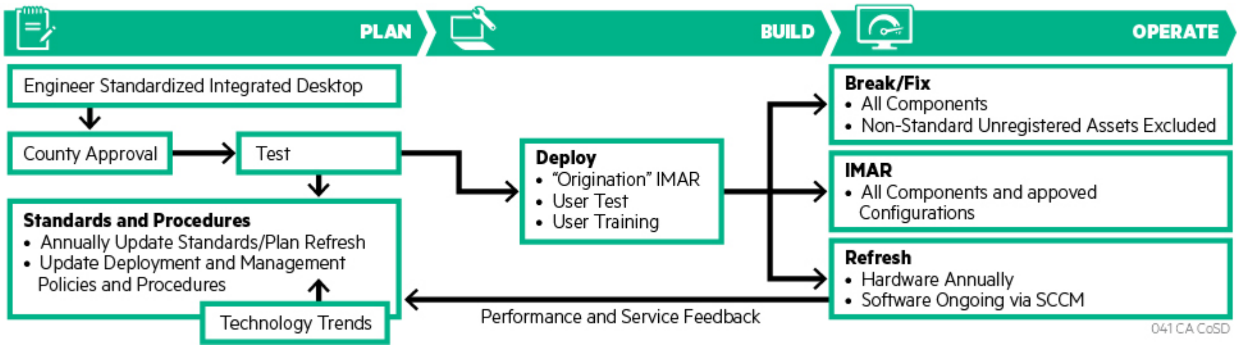
Generally, updates to the existing desktop environment, including hardware, core software, and OS, and all other components shall be organized as follows:

- **Standard Yearly Updates.** These are annual updates to the standard configurations for hardware and Core Software – the total “platform.” Concurrently with these updates, hardware equipment that is due for tech refresh shall be scheduled so that all changes are made as one event.
- **Ongoing Updates and Refresh.** This activity entails ongoing, incremental, regular updates to approved configurations. Ongoing updates relate primarily to software. Contractor shall check the hardware inventory annually to determine which machines are eligible for refresh.
- **Ad hoc and Emergency Pushes –** Emergency pushes shall be event driven. Typically, these are defensive security pushes in response to vendor patches to protect the security posture of the standard desktop configuration and/or minor functional updates from the software OEM (versus major version upgrades, which shall be assessed more thoroughly and shall be part of the standard yearly update).

The figure below shows the Plan, Build, and Operate life cycle.

Enterprise Architecture and Desktop Engineering shall collaborate on changes to the standards—Desktop Engineering shall build and tests those changes and provide updates to the knowledge base and End User Service technicians via documented procedures and cross-training sessions.

End-User Services Framework


PLAN
BUILD
OPERATE
Engineer Standardized Integrated Desktop
County Approval
Test
Standards and Procedures
• Annually Update Standards/Plan Refresh
• Update Deployment and Management Policies and Procedures
Technology Trends
Deploy
• “Origination” IMAR
• User Test
• User Training
Break/Fix
• All Components
• Non-Standard Unregistered Assets Excluded
IMAR
• All Components and appoved Configurations
Refresh
• Hardware Annually
• Software Ongoing via SCCM
Performance and Service Feedback
041 CA CoSD

Standardization and Governance

The cycle for standards governance and standard desktop configuration updates shall be annually.

Standards shall be updated based on a County request, Contractor’s assessment of the technology market, vendor presentations to the County, or other County initiatives. All requests shall be reviewed and consolidated. Contractor’s engineering group shall lead the consolidation and analysis of these requests and bring the County a consolidated list of recommendations, which shall be presented to the Governance Review Board for approval. Once Contractor has received the County’s approval, Contractor shall perform more detailed engineering and testing of the new configurations.

Process to Review and Approve Annual Updates to Standards. Major updates to the standard configurations and core software shall be made yearly, with a monthly rhythm. The timeline for annual updates to the standard configuration is shown in the table below.

Monthly Flow of Annual Standards

TIMEFRAME (MONTH TO MONTH)	ACTIVITY
Ongoing (January through December)	County performance trend analysis Industry trend monitoring User needs analysis
September through October	Current industry product assessments by Contractor team Vendor briefings to the County and Contractor
October	Draft updates to standards Review and approve new standards Update timelines/roadmaps
November through December	Perform desktop/core software testing and Systems Integration Test (SIT) Perform applications User Acceptance Test (UAT)
January through December	Deploy all tech refresh – annual updates based on device type and End-User-specific configurations Deploy software refreshes via SCCM

- Governance: Sponsored by the County CIO
- County participants include CIO and staff, and End-User representatives of each functional organization.
- Contractor participants include the COO, Account Chief Technologist, Technology Office Lead, Desktop Services Management, Applications Lead, and appropriate members from those organizations.
- Boards and Review Committees exist for Standards and Catalog management—such as the Configuration Governance Board (CGB) and Catalog Review Board (CRB).

Between the annual cycles and standards governance events, the Contractor's Technology Office shall host weekly Enterprise Architecture meetings with the County that review new technology trends, vendor roadmaps, and as needed, performance issues in the County environment. These meetings shall provide ongoing input once a configuration is fielded regarding immediate and/or systemic issues and provide a safety net to the annual engineering and testing cycle.

Engineering

Desktop Engineering shall be involved before and after standards are set up front with Enterprise Architecture to ingest new requirements, review new and emerging technologies, assess integration compatibility with current and fresh configurations, and recommend new standards. As new standardized configurations are rolled out, Desktop Engineering shall resolve Tier 3 tickets and systemic issues. The functions of Desktop Engineering, Integration Engineering, Enterprise Architecture, Applications Management and Operations, as well as Applications Development, IT security, and County business application owners shall work together to standardize and test desktop configurations and applications.

Major changes in hardware, operating systems, or other significant architecture upgrades shall receive more extensive engineering and testing.

Systems Integration and User Acceptance Testing. The Desktop Engineering group shall perform SIT and UAT testing using the test lab at the Rancho Bernardo facility. This test lab has multiple device types and configurations to test against to confirm that configurations are ready for deployment. The Desktop Engineer shall conduct SIT with the Test Engineer when images are updated and created to make sure the image and software work properly. Test results shall be peer reviewed and any issues shall be resolved before production deployment. For major upgrades Contractor shall perform full regression testing – End-User, performance, and security – as part of SIT and UAT.

UAT shall be performed by both Contractor and County users on both types of applications. It shall be performed when an application is first requested and approved, and when there is a major upgrade to the core software and OS standards.

Overall, this methodology results in a new gold image for new deployments and an upgrade path/procedures for current desktops that may or may not require re-imaging the desktop depending on the scale and scope of the upgrade.

This methodology shall be governed by County procedures.

Specific Support to Business Applications.

Contractor shall have an End-User representative for each application. Contractor shall also have an entire Applications organization that shall be responsible for applications and their support.

There shall be two types of applications:

- Catalog Applications – Catalog applications shall typically be COTS; they shall be limited to 440. Contractor shall monitor the number of applications to control County expenses. Contractor shall continuously work with the County to help optimize the applications list. Catalog applications do not have backend infrastructure associated with them – they are software packages, typically off-the-shelf. They shall be installed on the desktop and have no interaction with any other components (i.e., no database or servers it needs to talk to).
- Portfolio Applications - Portfolio applications shall be supported by the Contractor applications team and shall typically be hosted in the data center, on a two-tier or three-tier architecture (thus servers and databases are involved, along with a desktop client most of the time). With Portfolio applications, the project team (more than just desktop engineering, to include the DBA and application SMEs) shall be involved in SIT before it goes to UAT.

Some portfolio applications (e.g., Kronos) require unique configurations or n-1, n-2 desktop configurations that are not the current standard. Contractor shall accommodate these needs on a case by case basis. Contractor shall work with the County to improve the standardization of these exceptions.

Desktop Computing refresh activities as well as maintenance and upgrades to the Desktop Computing Core Software, including the Operating System.

Contractor shall update the existing desktop environment as follows:

- **Standard Yearly Updates.** Annual updates to the standard configurations for hardware and Core SW. Concurrently with these updates, hardware equipment due for tech refresh shall be scheduled for refresh.
- **Ongoing Updates.** Ongoing incremental, regular updates to approved configurations. Ongoing updates shall relate primarily to software.
- **Emergency Pushes.** Event-driven, defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which shall be assessed more thoroughly and are part of the standard yearly update).

Contractor shall only perform refresh activities which either 1) have passed the configuration control and governance processes to become part of the standard configuration, including having been assessed for cost/risk/benefit; or 2) are emergency in nature and have been approved through a streamlined process.

Hardware Refresh. Contractor shall have a group dedicated to refresh that shall travel the County, working from the refresh list, focusing on one site at a time to minimize disruption.

Software Refresh – Software/SCCM.

Contractor shall use System Center Configuration Manager (SCCM), previously known as SMS, to automate refreshes and updates and manage the overall deployed configuration. SCCM shall prevent users from installing un-authorized software or authorized software in unauthorized configurations.

Software refresh shall include updates to the OS and applications.

SCCM

Contractor shall provide SCCM 2016 and the following core capabilities for the County:

- Software distribution – by End-User, by machine; mandatory and optional (self-service)
- Asset intelligence – hardware and software inventory, compliance, application usage tracking
- Hardware and software updates – firmware and security updates
- OS deployment – for workstation only
- Mobile device management

SCCM 2016 shall be introduced into the Library environment to maintain currency of and distribute software to the devices on the Library network with the enterprise standard tool.

Using SCCM, non-emergency software refresh shall be performed outside core hours, usually at 2:00 a.m.

Major software and OS version updates (e.g., from Windows 7 to 10) shall be considered changes to the standard configuration and shall be managed as such. For major OS upgrades, the methodology is more extensive and may include re-imaging the disk.

Requests for Change (RFCs) shall be used to document a change to the environment. Updates may be applied as a push change and documentation shall remain in the knowledge repository of the End-User Services. The RFC shall remain in the CRCB document repository.

Contractor shall adhere to the County Microsoft Windows Non Security Updates Process document. Contractor shall follow overall architecture, desktop, and LAN/WAN security practices, using tools described below.

For security-related updates, in addition to the steps above, the security office shall review and validate the security updates. Urgent updates shall be pushed out on an accelerated schedule—either that night or immediately—in accordance with streamlined emergency approval process.

Approaches, processes, and procedures are governed by County procedures.

Operations and Maintenance of Core Software, including OS.

Desktop Engineering shall have procedures for maintaining the OS image and core software. On a quarterly basis, new device drivers shall be tested for items such as printers and network interface cards and added to the OS image. Security and non-security updates shall also be added quarterly to the OS image to facilitate a faster imaging process. Core software shall be updated during the year with minor revisions, to address vulnerability issues with the browser, for example. Major revision upgrades of the Core software and OS shall be addressed via updates of standards that are approved by the County and executed as projects.

Maintaining an up-to-date (Core Software) Desktop Computing environment

Generally, updates to the desktop environment, including hardware, core software and OS, and all other components, shall be organized as:

- **Standard Yearly updates.** These are the annual updates to the standard configurations for hardware and core software. Concurrently with these updates, hardware equipment that is due for tech refresh shall be scheduled for refresh.
- **Ongoing Updates.** This is ongoing incremental regular updates to approved configurations. Ongoing updates shall relate primarily to software.
- **Emergency pushes.** Emergency pushes shall be event driven. Typically, these are defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which are assessed more thoroughly and are part of the standard yearly update).

SCCM.

To maintain the core software configuration, Contractor shall use SCCM (previously SMS) to automate refreshes and updates and manage the overall deployed configuration. In addition, SCCM shall control and identify users installing unauthorized software or authorized software in unauthorized configurations.

The software distribution process shall be as follows:

Software Distribution Process

- The County approves the core software standards and configurations.
- Desktop Engineering (DE) posts completed Software Distribution templates to the DE SCCM Production Requests SharePoint site and informs SCCM Ops.
- The SCCM Ops team lead reviews the document for accuracy or any issues.
  - If issues found, he notifies DE and requests update/correction.
  - If no issues found, he sends notification to the SCCM Ops team and applicable desktop engineers that it is approved for production distribution.
- SCCM Ops team member is assigned to perform the setup in the SCCM console.
- SCCM Ops team member sets up the software distribution as specified in the document.
- SCCM Ops sends notification to SCCM Ops team and applicable desktop engineers that setup is complete and includes details of the setup and a link to the advertisement status report for the new advertisement.
- After the advertisement start/mandatory time, SCCM Ops monitors the advertisement status to help identify and correct problems with distribution.

End-User computer devices shall be locked so users cannot perform their own installs.

Performance or systemic issues on desktops

For enterprise-wide systemic issues in the desktop environment, Contractor shall use ITIL Problem Management to identify the root cause and to drive remediation. Steps shall include:

- Treat performance and systemic issues as cross-functional problems in that they involve desktop services, engineering, asset management, etc.
- Use data from tools (such as Riverbed, Cascade and APM), users, and tickets.
- Perform analytics; look for patterns and trends.
- Isolate a problem or determine a pattern of the same problem, then attempt to replicate the problem in Contractor's test lab so that Contractor can conduct deeper diagnostics.
- Promptly escalate and involve vendor support channels as needed.
- Identify the error and generate RFCs, either to configurations and/or service standards depending on the problem.
- Depending on the nature of the problem and the solution, it may be an emergency push or bundled with a regular release.

- If the root cause of the problem is with the core software configuration, Contractor shall go through the appropriate engineering and testing process to correct the error, gain the County's approval, and change the standard.

At the deskside level, if Contractor finds that there are multiple incidents, or troubling trends, Contractor shall enlist Problem Management to find the root cause and remediate it.

Specific Issues. For any issue, Contractor shall identify it, resolve it, identify the root cause, and then modify standards and/or procedures to prevent the issue from occurring in the future.

Contractor shall have effective processes in place to identify systemic issues that involve human feedback, trouble ticket data analysis, and system performance data. Contractor shall have a rigorous process to promptly address the root cause of systemic issues.

Engineering desktop software and Constant Improvement of quality and timeliness of applications and software package delivery to End-Users.

Service to the User.

Contractor shall involve the End-User and provide the End-User a voice and authority during each phase of Contractor's approach.

Plan

- An End-User shall be able to initiate a request via the Service Portal for new software or applications or support to existing software or applications
- Users, Group IT Managers, CTO, and Contractor Applications team representatives shall be involved in the annual standards refresh along with Enterprise Architecture and Desktop Engineering
- Users, Group IT Manager, CTO and Contractor Applications team representatives shall be involved in the weekly Enterprise Architecture meetings with Desktop Engineering
- Users shall help specify and conduct End-User acceptance testing (UAT)
- Applications shall be tested both by Contractor (first) and the sponsoring End-User

Build

- User manuals, FAQs, and other supporting reference material shall be configured and deployed.
- User feedback from prior similar deployments shall be incorporated

Operate

- User shall receive an introduction deskside to new equipment and software
- Various types of End-User training shall be available depending on the nature of the software and applications
- User service shall always be available via the Service Desk

Desktop Engineering

Requests for packaging software for the desktop shall be made through catalog requests or project requests from the County. As such, Desktop Engineering shall create the installation package, test it in the engineering lab, peer review it, and provide it to the client to conduct UAT, in the case of a catalog request or the Contractor Applications team for testing, in the case of project/portfolio requests. Upon successful Applications team testing, client UAT shall be conducted. When client approval has been obtained, Desktop Engineering shall submit the request to End-User Services – SCCM Ops for production deployment.

Performance Monitoring – HES shall monitor the performance of the applications and hardware devices as part of the overall enterprise. When there is a reason for deep applications performance monitoring or any kind of additional performance monitoring, Contractor shall perform troubleshooting and analysis using the tools and teams that Contractor discussed previously in this section. The addition of the analytics data warehouse that Contractor puts in place shall pull together the complete view of the information and data that Contractor has within its systems.

Performance Tuning **-** When applications need tuning, Contractor shall work cooperatively with the application vendor and the Contractor Applications team.

Continuous Improvement

When MASLs identify a process quality issue, Contractor shall implement CSI following the standard Deming Cycle (Plan/Do/Check/Act). Contractor shall on a continual basis seek to improve End-User services by identifying improvement areas, planning and implementing remediated items, and measuring the change in Contractor's quality metrics.

Quality and timeliness of delivery

The quality of desktop performance shall be constantly assessed at many levels.

Quality of Applications. Quality of applications and their hosting shall be tested as the application is approved for the standard configuration or OIPC. In addition to Contractor-performed SIT and UAT, the hosted application shall be tested by the sponsoring End-User. Finally, the applications in the configurations shall be tested by service technicians when an IMAR or refresh action warrants.\

Timeliness of Software Package Delivery.

Contractor shall proactively work throughout the process to facilitate the speed with which users can obtain new applications and the speed with which they can supported. Applications shall go through the Plan, Build, and Operate process.

Plan.

Contractor shall work closely with the County during each step so each application request is prioritized correctly. Contractor shall use the GR, CRB, and weekly Enterprise Architecture review meetings as forums to achieve this. Applications shall be tested both by Contractor (first) and the sponsoring End-User. Some packages require legacy configuration of the standard desktop.

Build.

Once an application is approved, during the Build phase, Contractor shall address engineering issues on a case by case basis and work cooperatively with the application owner.

Operate.

As applications are released as approved and are part of OICP, all standard procedures shall apply. Applications operational issues shall be resolved at the highest possible tier, but some applications are specialized and complex. Applications escalation shall be a Tier 3 item.

4.5. Desktop Computing Services

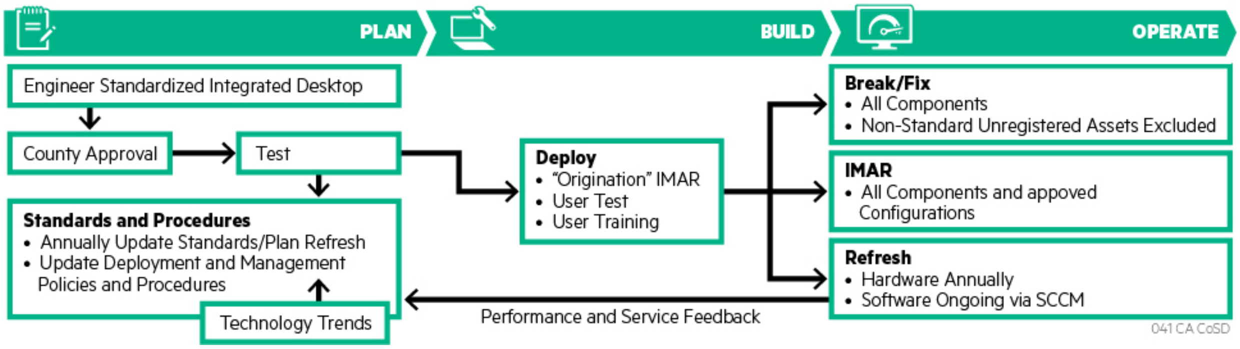
4.5.1. Process and Procedures

- Solution to meet the requirements

Contractor's Desktop Computing Services framework solution shall integrate all required components of End-User Services, interfacing components (such as Service Desk) and cross-functional components (such as Asset Management). The figure below illustrates Contractor's integrated framework.

Contractor shall use the existing framework methods throughout the transition for a smooth and reliable process. The framework shall be driven by the "plan, build, operate" concept, as illustrated in the figure below.

Desktop Computing Services Activities across the Plan, Build, Operate Lifecycle

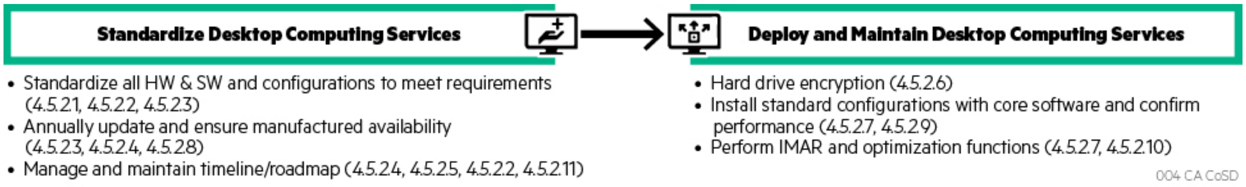

PLAN
BUILD
OPERATE
Engineer Standardized Integrated Desktop
County Approval
Test
Standards and Procedures
• Annually Update Standards/Plan Refresh
• Update Deployment and Management Policies and Procedures
Technology Trends
Deploy
• "Origination" IMAR
• User Test
• User Training
Break/Fix
• All Components
• Non-Standard Unregistered Assets Excluded
IMAR
• All Components and appoved Configurations
Refresh
• Hardware Annually
• Software Ongoing via SCCM
Performance and Service Feedback
041 CA CoSD

Contractor shall manage the desktop services and architecture as an integrated solution across the Plan, Build, Operate life cycle structure.

Rationale for Choosing This Solution

This solution shall provide standardization as a key component to optimizing service (see figure below). The bulk of Contractor's efforts shall focus on enhancing Contractor's services to the County— best accomplished by standardizing a set of technologies that recognize the diversity of the employee base and also derive support, cost, and efficiency benefits.

Desktop Computing Services Solution


Standardize Desktop Computing Services
• Standardize all HW & SW and configurations to meet requirements (4.5.2.1, 4.5.2.2, 4.5.2.3)
• Annually update and ensure manufactured availability (4.5.2.3, 4.5.2.4, 4.5.2.8)
• Manage and maintain timeline/roadmap (4.5.2.4, 4.5.2.5, 4.5.2.2, 4.5.2.11)
Deploy and Maintain Desktop Computing Services
• Hard drive encryption (4.5.2.6)
• Install standard configurations with core software and confirm performance (4.5.2.7, 4.5.2.9)
• Perform IMAR and optimization functions (4.5.2.7, 4.5.2.10)
004 CA CoSD

Key: Numbers are Exhibit H SOW Requirements. (e.g. 4.5.2.x)

- Deployment plan for resources and use of facilities

Facility Approach. Desktop Computing Services shall provide by a Contractor services team located centrally at Contractor's Rancho Bernardo facility. Additionally, Contractor shall have embedded support technicians at the COC and CAC.

- 1 employee shall reside at the COC
- 2 employees shall reside at the CAC

As service issues require in-person support, Contractor shall deploy technicians from Contractor's regionalized End-User support team. Most site technicians shall reside at Contractor's Rancho Bernardo facility. The technicians shall use this as their home base, traveling to any of the County sites with the equipment and tools required.

Contractor shall staff the core hours of Monday through Friday 6:00 a.m. to 6:00 p.m. with a full shift. Non-core hours shall be staffed at levels sufficient to provide necessary service as required over the weekends, on holidays, and after the business day. Contractor's support service levels shall be available 24x7x365. Online ticket creation shall be available with the Service Desk 24x7 via the Service Portal, phone call, or chat, so even non-urgent service tickets can be logged anytime.

How Desktop Encryption shall be conducted, measured and reported:

1. Conducted: An Contractor recommended, and County approved Standard PC, Standard Laptop and Engineering Workstation Hard Drive Encryption solution, (e.g., Symantec EndPoint Encryption) shall be installed on all Standard PC, Laptop and Engineering Workstation as part of the Core Application Suite prior to delivery to end-users. The approved solution shall be maintained at current vendor version. The Hard Drive Encryption solution shall be installed on all County assets by certified Contractor Services Technicians, or remotely via SCCM. If installed remotely, a successful install shall be verified/QA'd by Contractor prior to deployment and/or turnover to End-User.

2. Measured: The Reporting Console for the Hard Drive Encryption solution shall be the primary tool utilized to identify any Standard PC, Laptop and Engineering Workstation not reporting a successful install of the approved Hard Drive Encryption Solution. Other tools such as SCCM may also be utilized to identify compliant/non-compliant devices. Regularly scheduled electronic scans of all County connected devices in the environment by the Reporting Console shall be the primary tool to measure the quantity of encrypted and non-encrypted devices on the Network. All non-compliant assets shall be scheduled for remediation and/or repair by End User Services.

3. Reported: At requested scheduled intervals, the Reporting Console for the Hard Drive Encryption Solution shall generate a report of all assets by asset tag number that are reporting as compliant and/or non-compliant. The Report shall identify each asset by asset tag and the present version of the Encryption software installed. This report shall be provided to the County and posted on the County Service Portal.

How Desktop Optimization shall be conducted, measured and reported:

1. Conducted: Contractor shall perform optimization analysis daily using Contractor's automated tools that aggregate findings and establish trends that become the basis of Contractor's weekly reporting. Performance issues identified by monitoring or Incident Trending reporting or County escalation shall be investigated by Contractor Problem management team for Root Cause Analysis (RCA). RCA results shall be reviewed and provided to Contractor End User Services Engineering. Contractor End User Engineering shall identify and test solutions to resolve RCA findings and provide those findings to Enterprise Architecture.

2. Measured: Frequency and duration of issues shall be measured by Incidents reported in the HPSM tool.

3. Reported: Contractor shall report issues, findings and resolutions to the County and post on the Service Portal.

How Desktop Performance shall be conducted, measured and reported:

1. Conducted: Formal Desktop Hardware and Software Standards shall be reviewed annually to ensure that the Core Applications suites approved for the County are implemented. Contractor recommended changes to Hardware Standards and Software Standards (e.g. New and or modified existing Resource Units; updated Core SW Versions) shall be tested by Contractor for compatibility, functionality, and performance with the existing approved Core Software suite.

2. Measured: Performance shall be measured by tools such as Cascade and the Application Performance Management suite.

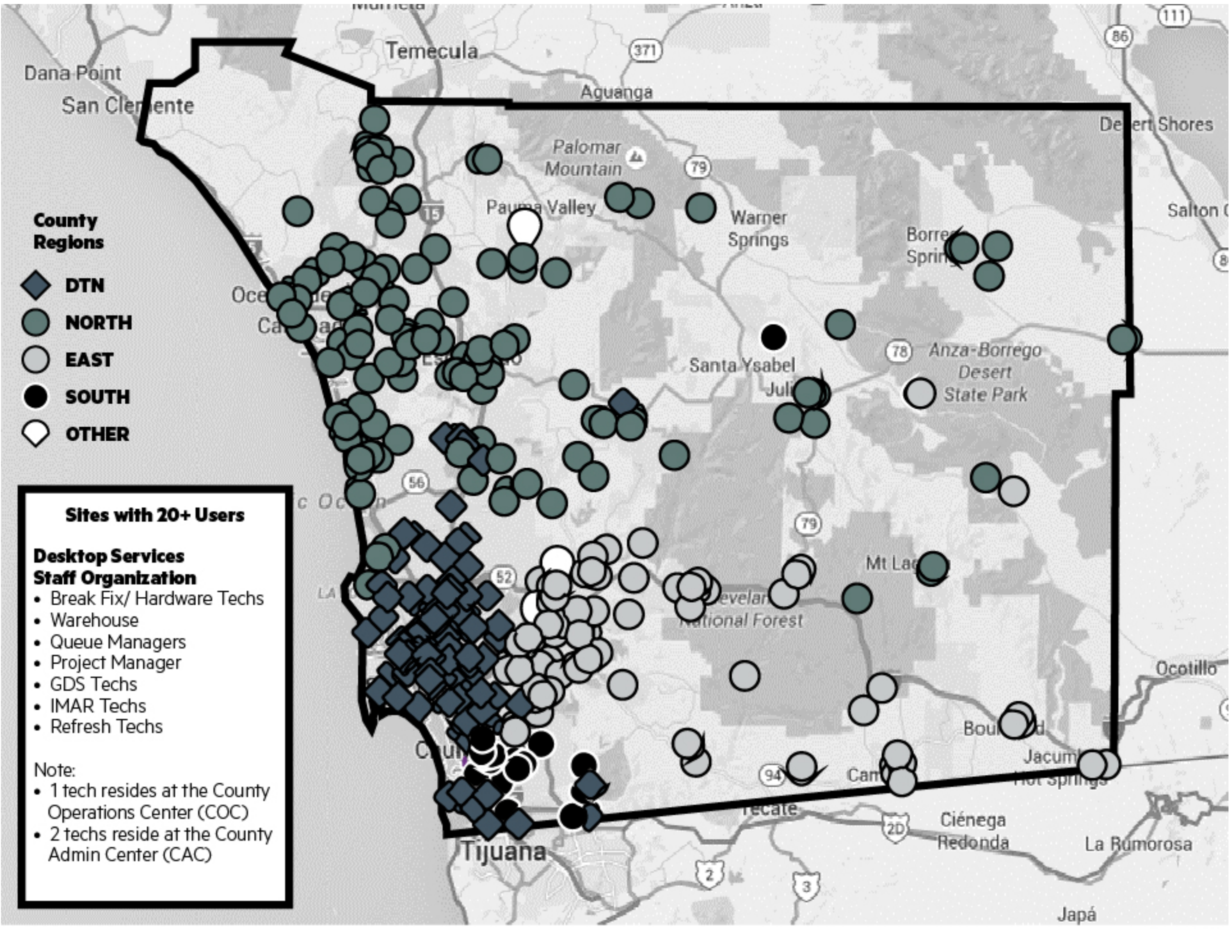
3. Reported: Monthly Reports shall be provided to the County and posted on the Service Portal.

Service Management. To serve all the sites that do not have dedicated onsite support, Contractor shall have a functionally organized technical support team. This team shall travel in a fleet of vehicles, each of which is provisioned with spare parts and "hot swap" spares to provide "first-touch" issue resolution where possible. After assessing the problem, Contractor's technicians shall have the necessary troubleshooting skills and shall be empowered to restore End-User service quickly. Contractor shall then take the faulty equipment back to the warehouse for more extended diagnostics and repair.

Service Scheduling. Service technicians shall provide numerous types of service, including break/fix ticket requests, IMAR actions, or software refresh. Hardware and core software configuration refresh actions shall be planned for implementation throughout the year. IMARs shall also be planned in advance and are non-emergency. For event-driven break/fix service, technicians shall be deployed by the queue manager based on the functional content of the ticket and the End-User's location. The figure below shows the geographic coverage of End-User support and summarizes the functional organization of End-User Services.

Emergency Management. In the event of a disaster or emergency, the Desktop Computing Services team, along with the framework teams, shall provide immediate services to the County. When the OES is activated, the service delivery manager (SDM) on call, along with the Infrastructure Operations Manager, shall immediately be dispatched to the County location with a desktop technician to provide the first shift of support. Contractor shall have a robust rotation of management and technicians that shall remain on site with County staff and other entities that are brought in to support the effort.

Functional and Geographic Organization of Service Staff



003 CA CoSD

When these events occur, Contractor shall work with the County to stand up Local Assistance Centers (LACs) strategically placed where the event has occurred. Contractor, along with AT&T, shall provide all the equipment, connectivity, and onsite staff to offer County employees everything they require. If the OES is not activated and a request comes in from a business group to provide support for a disaster, Contractor shall implement the same process and provide the same support.

Service Technician Skill Profile. The minimum skills and experience required for all technicians shall be as follows:

- Desktop OS (Windows 7, Windows 8.1), with mandatory Windows 10 training for all techs underway
- Basic level server hardware replacement skills
- Customer service skills
- Basic data backup skills
- Minimum 2-year remote and onsite troubleshooting experience
- Attention to detail
- Deskside End-User and technical communication skills

All technicians shall have the same base skills and shall be cross-trained so that, in periods of surge, Contractor can meet the service demand.

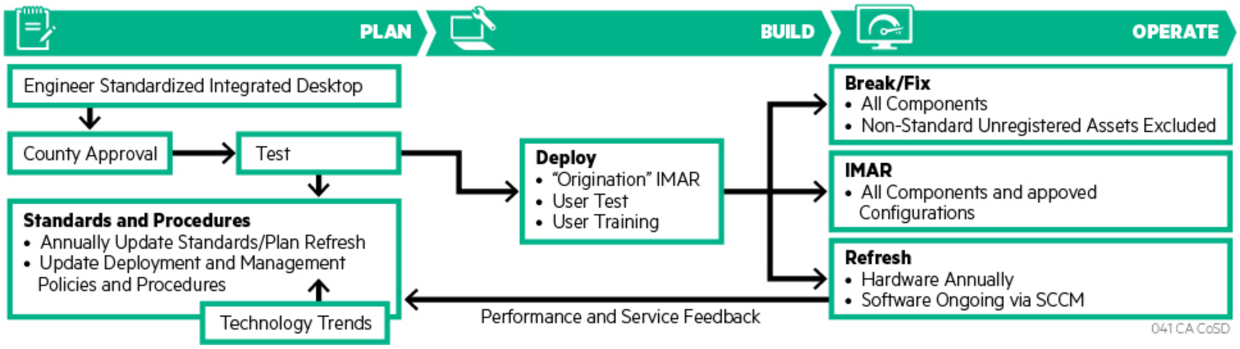
In addition, Contractor shall provide communications to Contractor’s service technicians to keep them up to date on the County’s mission via all-hands meetings, webinars, leadership briefings, weekly/monthly newsletters, knowledge shares, and other County specific activities.

Contractor’s service technicians shall be aware of Contractor and industry state-of-the-art and best practices via newsletters, webinars, the internal Contractor portal, team meetings, and so forth, for information about the latest technology, and for continuing education.

- Key methodologies and processes in solution including year-to-year continuous improvement

The following figure shall serve as a roadmap for Contractor’s Desktop Services Methodology.

Desktop Services Methodology


PLAN
BUILD
OPERATE
Engineer Standardized Integrated Desktop
County Approval
Test
Standards and Procedures
• Annually Update Standards/Plan Refresh
• Update Deployment and Management Policies and Procedures
Technology Trends
Deploy
• “Origination” IMAR
• User Test
• User Training
Break/Fix
• All Components
• Non-Standard Unregistered Assets Excluded
IMAR
• All Components and appoved Configurations
Refresh
• Hardware Annually
• Software Ongoing via SCCM
Performance and Service Feedback
041 CA CoSD

The **Plan Phase** shall include engineering, testing, establishing standards for desktop hardware and software, and obtaining applications approvals. The standard desktop configurations shall be re-assessed and updated annually with County review and approval. During this annual review, the technology may or may not change. Update decisions shall depend on complexity, End-User benefit, technical necessity, and County approvals. Contractor shall continue to bring full transparency and engineering rigor and review into the annual update process. The Optional Items Catalog (OIC) shall include non-standard items that the End-User may still require. In addition to supporting the current field equipment, the standards engineering function shall also include forward-looking work with vendors and the greater technology community to anticipate and plan for future incremental and transformative configurations. These shall be documented in the timeline/roadmap documentation and briefing to the County annually.

The Desktop Engineering organization shall maintain, update, test, and annually release the standard hardware and software configurations. Desktop Engineering shall work with Enterprise Architecture to integrate into the environment, and provide cross-training to the Operations team. This group shall coordinate engineering and testing prior to deployment to address and eliminate issues such as older drivers and network interface card (NIC) mismatches.

Contractor shall conduct a weekly Infrastructure Project meeting to discuss the current status of ongoing infrastructure-related projects in the environment. Enterprise Architecture meetings review, for example, new technologies, changes to the desktop hardware and software standard and technical requirements for a project.

The **Build Phase** shall include the full set of activities to assemble, deploy, and test each individual standardized unit (with approved options); these shall include desktops, laptops, tablets, printers, and other network resources in a standardized MS-Windows based environment. Contractor shall follow the following process:

- Upon receipt of the hardware, Contractor shall tag it and have it ready for imaging when needed.
- The machine shall be pulled from the warehouse, and prepared to be imaged based on the configuration requested.

- Once the image/applications are completed, validated, and tested, Contractor shall put the equipment in the warehouse, where it is kitted with all of the accessories, and shall ensure the device is ready for delivery.
- Service ticket documentation or communication from the refresh the project manager shall then tell the technician where and to whom to deliver the hardware.

Desktop Engineering shall create a custom enterprise operating system (OS) image for the County, which shall comprise the MS Windows operating system and device drivers. This custom OS shall be made available to the imaging technician who handles imaging for refresh, IMAR, break/fix. During the business day, Contractor shall have staff onsite in the Rancho Bernardo facility in the imaging room that can complete hot swap devices for loaners as needed, and copies of these images shall be provided to the technicians in the field for onsite re-imaging.

The **Operate Phase** shall include the maintenance, operations, refresh, IMAR, break/fix, and everything else to support daily operations for the End-User. Operations and support activities shall cut across the frameworks and integrate User Service functions from the Service Desk, such as ticketing and remote support; service management functions such as asset management, configuration management, and process improvement; and other components of the End-User Services framework. Generally, Contractor shall adhere to the following process:

- Ticket requesting action shall be received, logged, and dispatched to a technician.
- Technician shall perform the required action to resolve the End-User's issue in accordance with documented procedures and services standards.
- Functional operation of the hardware and/or software shall be validated by the technician before permission is obtained from the End-User to close the ticket
- User satisfaction shall be confirmed verbally and via the Customer Service Survey sent out at the closure of the ticket.
- Asset management database shall be updated, if required
- The ticket shall be closed.

Hardware and software not in the standard configurations, such as BYOD smartphones and standalone printers, shall be supported as non-standard items. Contractor shall have processes in place to support requests for service on these items on an as-requested basis.

The Desktop Computing Services component shall be used to integrate all components of the desktop configurations: hardware, software, applications, network print, communications and, MDM.

Scheduling

For the annual refresh requirements and schedule, Contractor shall make all reasonable efforts to complete all the equipment at a given location before moving to the next site. Communications shall go out at multiple points for each device to prepare the users and avoid as much disruption as possible on the day of refresh. A target schedule shall be provided on an annual basis to the identified points of contact (POCs) to review and make edits as needed. Contractor shall work with the County's IT coordinators directly, along with the CTO point of contact, so that if changes need to be made to locations and dates, Contractor can accommodate them to prevent disruption. Contractor shall have a dedicated project manager assigned to the refresh activities of the End-User devices to provide solid communication, consistency, accuracy, and delivery of services in this space. The project manager shall also be responsible for the overall status of the project plan created annually for each refresh cycle and shall report on that weekly in the Infrastructure Project meeting.

Refresh.

Technical refresh shall be performed on a rolling basis throughout the year based on equipment type, install date, and refresh timelines. There shall be a 6-month refresh availability window that shall start 6 months before the scheduled refresh date and a 2-month grace period after each refresh date. Contractor shall take these into account during refresh planning and optimization. Contractor may exceed the 6-month early refresh window based on County requirements.

In addition, the County may request an early refresh of a desktop computing asset through the IMAR process at any time out of normal refresh cycle. If the device is not in the current refresh schedule or the request date is greater than 6 months earlier than the normal cycle refresh date, the department shall be charged a pre-defined rate per month based on device type.

Desktop Computing Services shall have a team of refresh technicians who specialize in performing refreshes. The technical refresh process shall be as follows:

- At the beginning of the calendar year, a draft schedule shall be communicated to the County
- Contractor shall work with the County to around any County business events. Contractor shall then finalize the schedule with the County coordinator.
- Prior to performing planned work at a site, Contractor shall communicate with the coordinator to validate planned activity is still acceptable.
- A review of every device shall be completed 3 to 4 weeks in advance of the actual refresh to identify custom configurations, applications, standalone hardware requirements, replacement model, extra tray requirements, and so forth.
- Equipment, including software configurations, shall be prepared to the extent possible at the warehouse prior to delivery to the End-User based on the information from the pre-field form. This shall include hardware configuration, any hardware default settings, basic software imaging, and standard software configurations.
- Testing is performed.
- Communications shall be sent to End-Users and POCs during all required steps of this process to make certain that nothing is missed.

At the End-User site, Contractor shall back up configurations from the machine that is going to be replaced. Users shall be notified during pre-communication to move data off the devices and onto shared data locations. The technician shall transfer any data that resides on the device that is related to applications. The technician shall also offer up to 30 minutes his or her time to transfer data unrelated to applications as a part of the refresh scope of work. The following actions shall be performed by the refresh technician at the End-User's site:

- Disconnect existing hardware, noting and/or tagging anything End-User- or site-specific, unique or non-standard.
- Install new hardware in the standard configuration, noting and addressing anything End-User-specific.
- Restore End-User configurations onto the new equipment; re-establish network access and network configurations.
- Perform functional tests to demonstrate to the End-User that the refresh was successful. Troubleshoot any issues.
- Make the End-User aware of any new features/functions of the new configuration and equipment. Point the End-User to relevant frequently asked questions (FAQs) or training, if needed.
- Notify the refresh project manager that the refresh is complete.
- The refresh project manager updates the database and reporting measures as activities are confirmed completed by the technicians.
- Notify the Service Desk that the ticket is complete.

In addition to desktop hardware refresh, there shall be an ongoing stream of major and minor software updates. These updates shall be managed by SCCM and shall usually be automatic and transparent to the End-User.

Break / Fix / Hardware Technical Support

Break/fix services shall be event driven and triggered by a service ticket. Technicians shall manage service on the integrated desktop configuration, not just the hardware.

Queue Management. Within Desktop Services, the queue manager shall assign tickets to technicians. This function shall be performed via a process supported by MS Office tools for scheduling. Technicians shall be assigned in an optimal manner, based on a combination of technical requirements, urgency of the ticket, geography of the ticket, and the technical complexity of the problem. For High Response End-User service, Contractor shall make all reasonable efforts to assign a familiar and experienced technician the High Response End-User knows and trusts. When a problem requires desk-side support, Contractor shall use the following methodology:

- Ticket forwarded from Service Desk to queue manager
- Queue manager determines to whom to assign the ticket
- Ticket is assigned to a technician, and the technician is notified of the ticket assignment
- Technician travels to End-User and performs the appropriate diagnostic protocol for the identified problem

To diagnose the issue, generally technicians shall use tools such as HP Diagnostics Toolset, LogMeIn Rescue, SCCM, Active Directory (AD), MS OffCAT, AirWatch, and others, depending on the nature of the problem. Technicians shall have additional options available for more complex problems:

- Correct the problem at the deskside using break/fix troubleshooting procedures for the specific problem
- Get peer level technical specialist support to assist with problem resolution
- Escalate to a SME as appropriate
- Hot swap to a loaner
- Hot swap to a spare

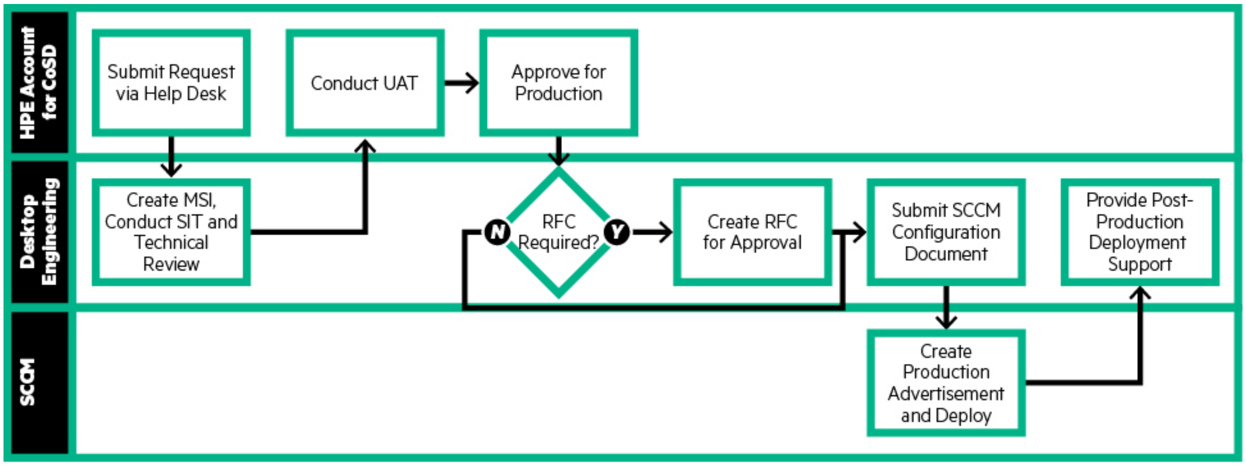
Technicians shall select the right method to get the End-User back in service as quickly as possible while still resolving the root-cause technical issue. The technician shall test and demonstrate to the End-User that the problem is fixed.

- The technician shall perform the foundational set of system and End-User testing, which is a series of standard tests.
- Technician shall log the fix, update the asset inventory (if necessary).
- Upon completion of the service, the technician shall move on to work their next ticket

IMAR

IMAR requests shall typically be triggered by non-urgent events. Any IMAR request that comes in with more than 25 items shall be considered a project and assigned within the End-User Service group to the project coordinator to manage and complete as required. The IMAR process flow, illustrated in the figure below, shall be the same as for all other types of requests.

IMAR Process


HPE Account for CoSD
Desktop Engineering
SCCM
Submit Request via Help Desk
Conduct UAT
Approve for Production
Create MSI, Conduct SIT and Technical Review
N
RFC Required?
Y
Create RFC for Approval
Submit SCCM Configuration Document
Provide Post-Production Deployment Support
Create Production Advertisement and Deploy

122 CA CoSD

HPE Asset Manager shall track all modifications to an asset record that are the result of moves (locations, users, and so on), adds (adding components), or changes (any other changes to the asset record). Modifications shall be tracked by field. If a field value is changed, HPE Asset Manager shall capture the name of the person making the change, the date of the change, and the name of the field that has been changed as well as the previous field value.

Moves, adds, or changes to assets can also be discovered or confirmed through auto-discovery, using the DDMi (Discovery and Dependency Mapping Inventory) tool for consistency. Contractor shall also provide tools to automate software-related IMAR activities, including policy-based software management. An IMAR action can be for a complete desktop, laptop, or other device configuration or just a component. Overall, the IMAR process shall be as follows:

- Receive an IMAR ticket
- Travel to the site of the equipment/bring equipment to the site location for install
- If the equipment is onsite, complete the identification and validation of this equipment to make sure inventory numbers match the tickets and asset database
- Back up all relevant End-User data and configurations and other environmental settings if required
- Make the appropriate IMAR action as indicated in the request:
  - **Install.** The "origination IMAR" is a special case of installation. For the first installation, the equipment is new, newly refurbished, or wiped to a new configuration. Where Contractor is able, new configurations of equipment can be prepared in the warehouse with hardware configuration, the standard software image installed, and any End-User optional items installed. This preparation work shall ease the installation process at the End-User's desk. Then configuration to the End-User's environment—for example, preferences, network connectivity and printer connectivity—shall be completed.
  - **Move.** A move is similar to a remove and install, except that software installation does not need to be performed. For a move, the technician shall note the End-User's connections and configurations, power down the old equipment, minimize its disassembly but do enough disassembly to safely move the equipment, and then physically move the equipment to the new location. Once at the new location, the technician shall perform the necessary installation steps completing with reconfiguration of End-User-specific and site-specific parameters.
  - **Add.** An add is typically for a new piece of hardware or software. Procedurally, an add follows the same steps as an install.
  - **Remove.** Complete removal of equipment can happen when an End-User leaves the County or when the equipment they are using is refreshed. Upon removal, the technician shall shut down the equipment, making necessary logical and physical disconnections and take the equipment away. Removed equipment shall go through the warehouse for asset management and proper disposal. Hardware at end of life shall

be so noted in the asset management database and is donated to San Diego Futures Foundation (SDFF). Removals of software shall include an action to make certain that any active licenses that were originally obtained are returned to the licensing pool for reuse.

IMAR Testing. In all actions that result in retained or upgraded equipment, the technician shall validate via deskside testing that the End-User functionality is correct and End-User configurations are created and/or retained as appropriate. This deskside test process shall be similar to that described in break/fix.

Continuous Improvement.

- Using the Deming PDCA (Plan/Do/Check/Act), Contractor shall on a continuing basis seek to improve End-User Services by finding improvement areas, planning remediation and implementing them, and measuring the change in Contractor’s quality metrics.
- Contractor’s leading indicators of quality shall be the service levels measuring Contractor’s performance along with the Customer Satisfaction Survey data provided. The service levels and surveys are leading indicators of quality, but Contractor also has all the data and analytics about the installed configurations and break/fix trends such as types of tickets, hardware configurations involved, system performance to ensure maximum optimization of the desktop environment, the nature of problems, and time to repair metrics.
- Contractor shall analyze these indicators to determine if Contractor needs to embark on a Service Improvement Plan to improve Contractor’s quality. These efforts shall be tracked, and the team recommends improvements. After putting them in place, Contractor shall then monitor closely both the incident and problem trends and their impact on Contractor’s service level performance.

During the Cross-Functional Transition, Contractor shall implement Microsoft SQL Server Business Intelligence to begin the process of building a reporting data warehouse, thereby bringing more automation and continuous improvement to the reporting process.

While the initial focus is on supporting SLA Reporting, the data warehouse shall provide a central repository that can support other ITSM analytic scenarios. Contractor is committed to continuous improvement and, over time, Contractor shall work with the County to extend both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. Benefits to the County can be measured through increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

The four specific areas of focus shall be:

- Service Strategy and Improvement Analytics: This area shall focus on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, Contractor can conduct analysis to reduce business impact of events, incidents, and problems.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

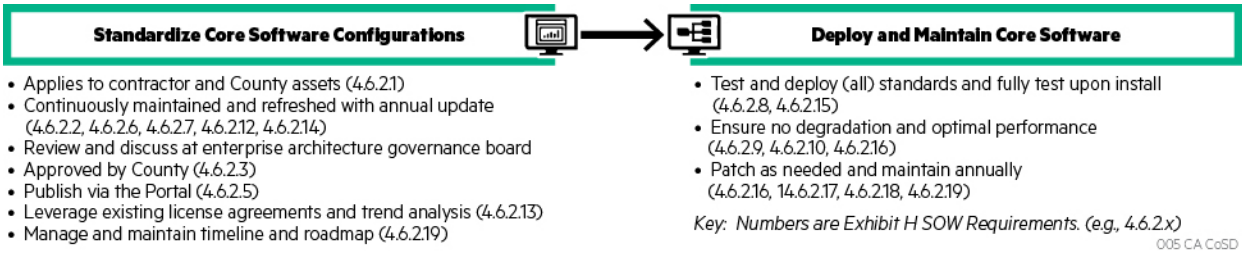
4.6. Core Software Services

4.6.1. Process and Procedures

- Description of solution to meet the requirements

Core Software Services shall be responsible for standardizing, describing, deploying and supporting a standardized and fully tested image onto all desktop assets including county retained assets. The fundamental activities of Core Software Services can be described as Standardization Management activities and Deployment and Maintenance Support activities, as shown in the figure below.

Core Software Service Solution



Standardize Core Software Configurations

- Applies to contractor and County assets (4.6.2.1)
- Continuously maintained and refreshed with annual update (4.6.2.2, 4.6.2.6, 4.6.2.7, 4.6.2.12, 4.6.2.14)
- Review and discuss at enterprise architecture governance board
- Approved by County (4.6.2.3)
- Publish via the Portal (4.6.2.5)
- Leverage existing license agreements and trend analysis (4.6.2.13)
- Manage and maintain timeline and roadmap (4.6.2.19)

Deploy and Maintain Core Software

- Test and deploy (all) standards and fully test upon install (4.6.2.8, 4.6.2.15)
- Ensure no degradation and optimal performance (4.6.2.9, 4.6.2.10, 4.6.2.16)
- Patch as needed and maintain annually (4.6.2.16, 14.6.2.17, 4.6.2.18, 4.6.2.19)

Key: Numbers are Exhibit H SOW Requirements. (e.g., 4.6.2.x)

005 CA CoSD

Core software configuration and updates shall undergo component testing, System Integration Test (SIT), regression testing, and User Acceptance testing (UAT) by the Contractor Technology Office, Applications Office, and Desktop Services organizations. Testing shall be both technically focused and End-User “use-case” focused. Testing shall also validate the security strength and integrity of the core software configuration and install.

Standards Enforcement and Exceptions.

Contractor shall use a process to regularly verify software versions and update as needed using SCCM, which shall scan the installed base of equipment for unauthorized programs. These checks and software updates shall be performed automatically over the network during off-hours.

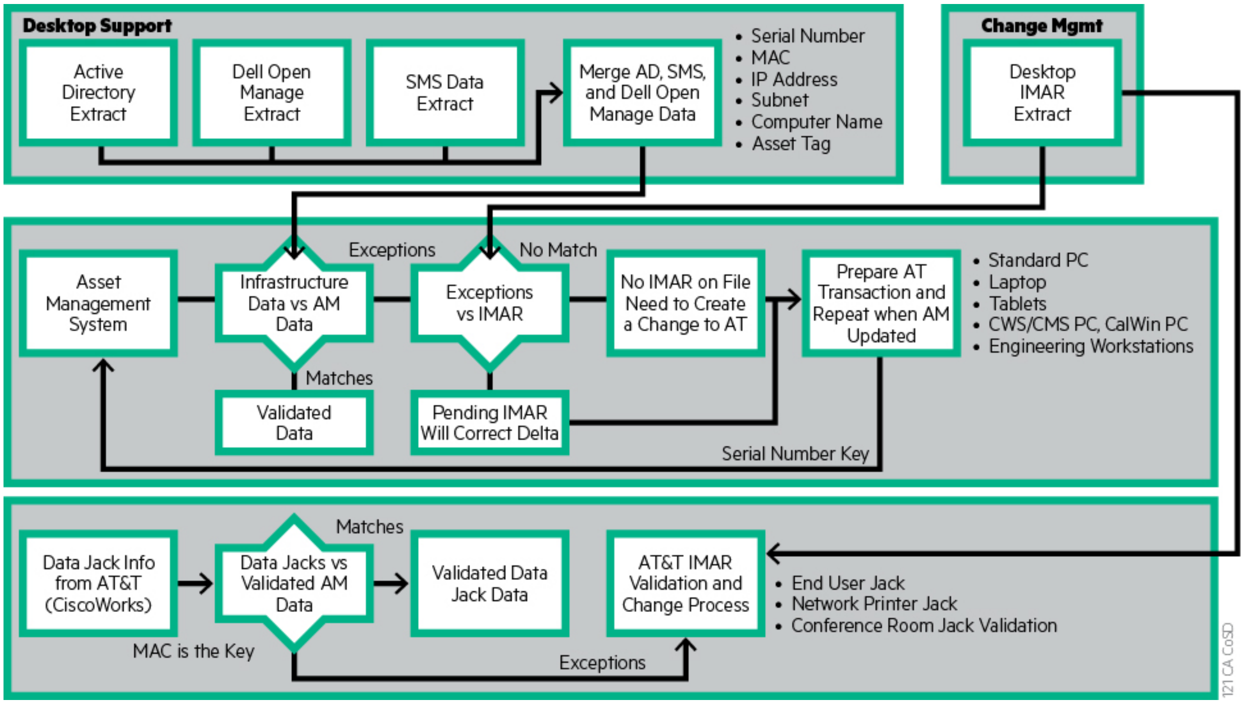
Contractor shall maintain a request process and adjudication process for non-standard items. The standard test shall be whether a business function cannot be performed with the standard configuration—not just that the End-User prefers a different tool. Users shall have FAQs, training, videos, and other tools available to them from the Service Portal to help them learn standardized tools. The End-User Services Manager along with the Service Desk Manager shall ensure all FAQ’s and documentation related to the End-User environment is kept up to date on the portal and that as new applications and hardware are implemented the appropriate documentation is put in place as required.

- Deployment plan for resources and use of facilities

The Resource and Facility approach shall be the same as for Desktop Computing Services. In addition to the Desktop Service Technicians, this component shall rely on the Project Management Office, Desktop Engineering, and Testing teams. These people shall also be located at Contractor’s Rancho Bernardo facility.

- Key methodologies and processes in solution including year-to-year continuous improvement

Core Software Services Process Flow



Core Software Services shall follow a process similar to Desktop Computing Services (Plan/Build/Operate), as described above. Some aspects with unique characteristic are described as follows.

Integration and User Acceptance Testing. This function shall be performed by the desktop engineering team, using onsite lab devices. This lab shall have access to the County and Library networks, and shall have many device types including the current standards and approved exceptions. When a new custom OS image or a new software package is built, testing shall be performed in this lab via a peer review process—meaning another member of the Desktop Engineering team shall perform the test to make sure it installs correctly, without errors, etc., and provides feedback/results to the desktop engineer who created the custom OS image or software package. Upon successful integration testing, if this is a Portfolio application, the Contractor Application team shall be engaged to perform UAT. When Application team UAT is completed, the software application shall be provided to a small subset of County employees, who perform UAT as well. Upon successful completion of UAT, the software package shall be made available for production distribution to the intended End-User community via SCCM. If this is a catalog application, the County client who requested the application shall perform UAT and, upon approval, it shall be made available to the intended End-User community. If this is a custom OS image, upon successful SIT, the image shall be made available to the support teams via Microsoft Development Toolkit (MDT).

Desktop Computing Refresh – Software/SCCM. System Center Configuration Manager (SCCM) shall be used to automate distribution of updates and to manage the overall deployed configuration. In addition, SCCM shall control and prevent users from installing unauthorized software or authorized software in unauthorized configurations.

Software refresh shall include updates to the OS and applications.

OS refreshes shall be treated as projects and are architected for little to no interruption in the County employee's daily work.

Using SCCM, non-emergency software updates shall be performed outside core hours, usually at 2:00 a.m.

For large OS upgrades within the year on a specific desktop, the software refresh methodology is more extensive and may include re-imaging the disk. Whenever possible, Contractor shall make reasonable efforts to bundle major software upgrades concurrently with hardware refresh equipment replacement as part of the annual cycle to minimize disruption to the End-User's work environment. Security Services for End-User Services shall be based on the defense-in-depth model.

4.7. County Retained Assets Services

4.7.1. Process and Procedures

- Description of solution to meet the requirements

County assets shall adhere to the same standards for configuration of hardware and software as all other assets. These machines shall be verified and enrolled just as all other assets. Then, County Retained Assets shall be serviced and supported using the same strategies, methodologies, procedures, resources, and facilities as contractor-provided assets. All appropriate service levels shall apply to standardized County Retained Asset Services.

When an End-User requests support on a non-standard item or non-enrolled item, the Service Desk or End-User support technician shall identify this situation using the asset database. If Contractor can support the non-standard item easily, Contractor shall do so as an act of immediate customer service on a case-by-case basis, with County approval.

- Deployment plan for resources and use of facilities

Since County Retained Assets that adhere to the standards and are enrolled are serviced the same as contractor-owned assets, the resource and facility approach to servicing these assets shall be the same as it is for Desktop Computing Services and Core Software Services.

- Key methodologies and processes in solution including year-to-year continuous improvement

County Retained Assets shall be managed the same as other assets and the solutions, methodologies, and procedures described elsewhere in this framework shall apply, depending on the nature of the required services.

County assets must adhere to the standard configurations, be “enrolled” to be on record as part of the managed configuration, and be recorded in the asset database. When contractor support is required to “build” the software configuration for County assets, this function shall be performed using the same standards and procedures as described in Desktop Services and Core Software Services. Once a standardized County Retained Asset is successfully enrolled, it shall be managed and serviced such as any other asset. Service tickets shall be flagged as “County Retained Assets” so that the technician knows of the hardware status just in case there is a troubleshooting problem related to the asset's origin.

Enrollment. In order to be serviced, a County Retained Asset must be enrolled in the Service Manager (SM) asset management database. At the time of enrollment, adherence to configuration standards shall be confirmed. Enrollment of County Retained Assets shall always verify by the Service Desk upon first service request.

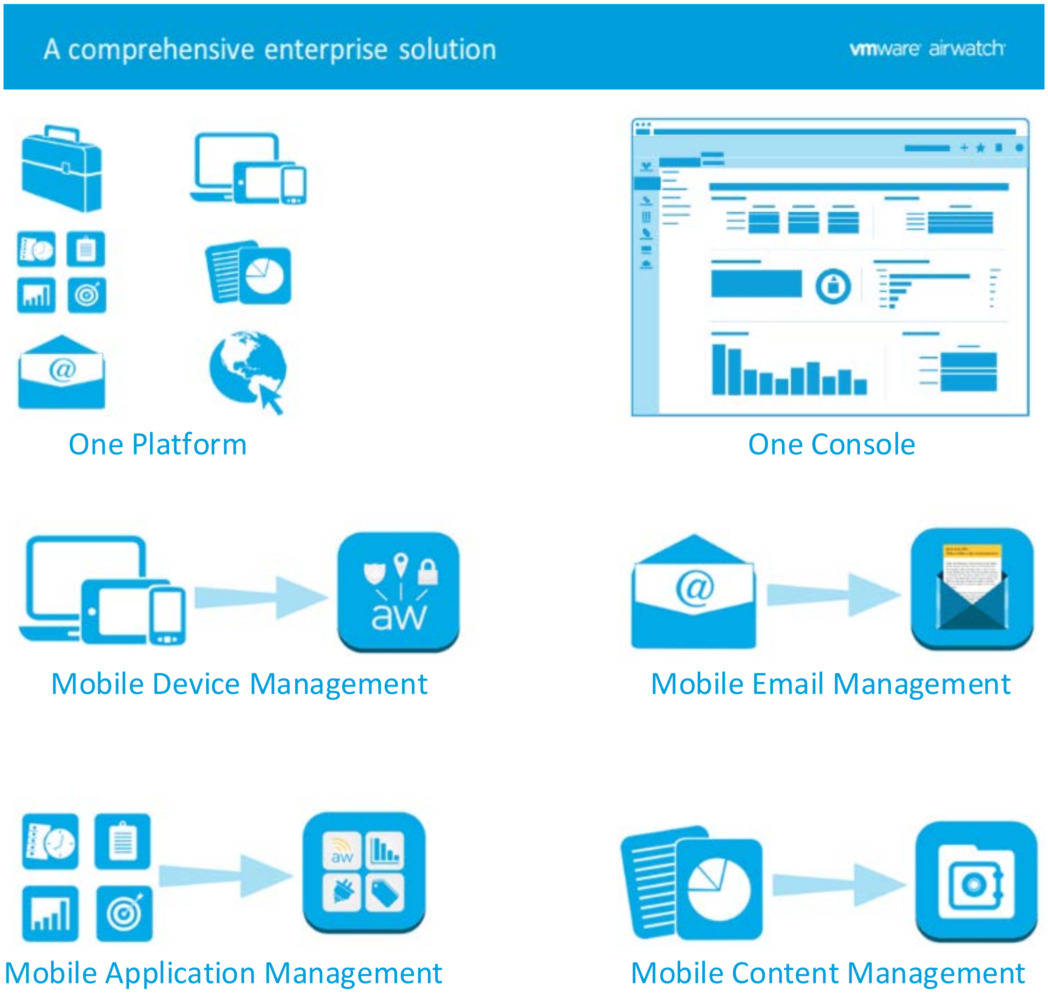
4.8. Mobile Device Support Services

4.8.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide the specific capabilities offered by the AirWatch platform, as shown in the figure below. All initial enrollment and other support requests shall be made to the Contractor Service Desk. The Service Desk shall validate the End-User's information and offer information and support that may solve the problem. For all mobile services that require AT&T support, the End-User's ticket shall get a "warm handoff" to the AT&T helpdesk. Contractor shall ensure that AT&T's helpdesk provides a single AT&T point of contact through each service transaction, even when AT&T needs to access multiple support organizations. Contractor shall ensure that AT&T support handles certain issues either by the local AT&T Incident/IMAR managers or by the AT&T Mobility Solution Services (MSS) and AirWatch partners. These End-User requests shall include Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Add/Delete Users, Device Enrollment (bulk or individual), and Device Wipe.

Capabilities Managed by the AirWatch MDM Solution


A comprehensive enterprise solution
vmware airwatch
One Platform
One Console
aw
Mobile Device Management
Mobile Email Management
Mobile Application Management
Mobile Content Management

To expand support, Contractor shall provide a fully managed Mobile Device Support Service that shall provide comprehensive operational support of all County-provided mobile devices as well as County resources that are available on BYOD devices. This service shall provide County users with single point of contact for AT&T’s MDM support, using a multi-tiered model designed to handle any type of mobility support need—mobile application, operating system, content management, device familiarity, email access, and even carrier related issues. The Contractor shall ensure that AT&T Enterprise Mobile Support team resolves AirWatch MDM, device/OS, and carrier-agnostic mobility issues in response to County End-User-generated trouble tickets logged with the Contractor Service Desk. This team shall provide expertise and support for most current mobile devices and accessories and shall directly engage the End-User in the diagnosis and resolution of their issues or shall route requests to the appropriate support organization if required. They shall also provide a “warm transfer” for County users for those issues requiring wireless carrier intervention. Throughout the process, this team shall also provide ticket management and communications through the Contractor’s Service Portal so that service levels are accurately tracked and the End-User is kept informed of the status of the request throughout its lifecycle. If the ticket requires further technical intervention, it shall be escalated through additional tiers of MDM support by AT&T.

The following is a summary view of each group’s responsibilities:

AT&T Enterprise Mobile Support Team

This group shall interact directly with the End-User on all MDM-related issues and provide the basic support and continuity of support for issues such as Device Enrollment, Device Lock and Wipe, etc. Additionally, this team shall provide general device and operating system support as well as facilitate warm transfer to the carrier as the need is identified. For the large percentage of issues, they shall provide first-call resolution. For the remainder of these tickets, they shall also act as the coordinator for the report if it requires escalation to one of the technical support organizations.

AT&T LCM Trade Street Service Desk

This group shall maintain overall responsibility for ticket management and service level attainment for MDM actions. As part of the ticket flow, they shall also provide the interface to Contractor for custom mobile application support, Active Directory, and Outlook email Exchange group issues.

AT&T Mobility Solutions Services (MSS) Application Service Desk

This Application Service Desk shall provide leveraged technical support to AT&T Enterprise Mobile Support team via phone, email, or internal AT&T portal for additional MDM support services. Responsibilities shall include advanced troubleshooting, isolation and resolution, application use, and configuration support as well as MDM managed services requests.

AT&T ASD/MSS Service Assurance Team

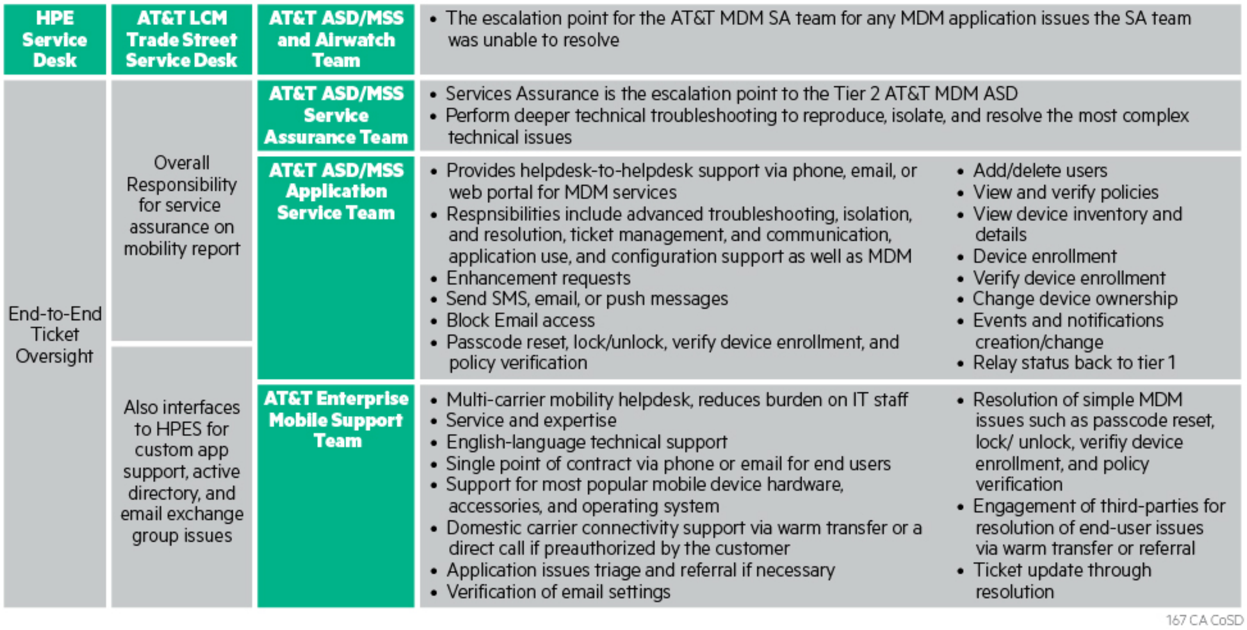
This is the first-level technical escalation point to the AT&T MSS Application Helpdesk, which shall perform deeper troubleshooting to reproduce, isolate, and resolve the most complex technical issues.

AT&T ASD/MSS and AirWatch Mobility Consultant Teams

This team shall serve as the escalation point for the AT&T ASD/MSS Service Assurance Team, which shall involve the AirWatch vendor technical team for any MDM application issues requiring the highest level of analysis and support.

The following figure provides more detail on the organizational roles for the mobile solution.

MDM Support Model



HPE Service Desk	AT&T LCM Trade Street Service Desk	AT&T ASD/MSS and Airwatch Team	• The escalation point for the AT&T MDM SA team for any MDM application issues the SA team was unable to resolve	
End-to-End Ticket Oversight	Overall Responsibility for service assurance on mobility report	AT&T ASD/MSS Service Assurance Team	• Services Assurance is the escalation point to the Tier 2 AT&T MDM ASD • Perform deeper technical troubleshooting to reproduce, isolate, and resolve the most complex technical issues	
		AT&T ASD/MSS Application Service Team	• Provides helpdesk-to-helpdesk support via phone, email, or web portal for MDM services • Respnsibilities include advanced troubleshooting, isolation, and resolution, ticket management, and communication, application use, and configuration support as well as MDM • Enhancement requests • Send SMS, email, or push messages • Block Email access • Passcode reset, lock/unlock, verify device enrollment, and policy verification	• Add/delete users • View and verify policies • View device inventory and details • Device enrollment • Verify device enrollment • Change device ownership • Events and notifications creation/change • Relay status back to tier 1
	Also interfaces to HPES for custom app support, active directory, and email exchange group issues	AT&T Enterprise Mobile Support Team	• Multi-carrier mobility helpdesk, reduces burden on IT staff • Service and expertise • English-language technical support • Single point of contract via phone or email for end users • Support for most popular mobile device hardware, accessories, and operating system • Domestic carrier connectivity support via warm transfer or a direct call if preauthorized by the customer • Application issues triage and referral if necessary • Verification of email settings	• Resolution of simple MDM issues such as passcode reset, lock/ unlock, verifiy device enrollment, and policy verification • Engagement of third-parties for resolution of end-user issues via warm transfer or referral • Ticket update through resolution

167 CA CoSD

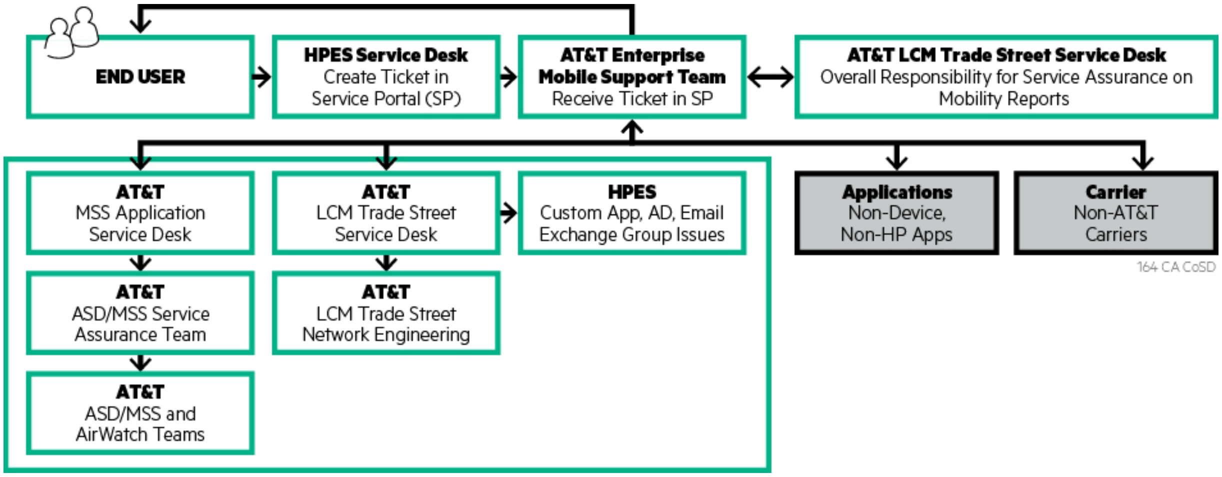
- Deployment plan for resources and use of facilities

Contractor shall leverage the local Life Cycle Management (LCM) team, the AT&T Enterprise Mobility Support team, and the AT&T Application Service Desk (ASD) organization. AT&T LCM personnel shall be located at the AT&T facility in San Diego. All other personnel and facilities shall be located at leveraged sites around the U.S.; this leveraged support shall be transparent to the End-User. The County's MDM infrastructure shall be hosted in the AirWatch shared cloud and shall interface with County resources through a geo-redundant AirWatch Cloud Connector configuration located at both the AT&T Point of Presence (POP) and the County Operations Center (COC). Smartphone users who are using BYOD shall have the option to get additional service related to their devices overall at their service provider's walk-in retail location, including AT&T locations for AT&T subscribers.

- Key methodologies and processes in solution including year-to-year continuous improvement

The same set of tools and processes used by the LCM Incident/IMAR desk shall be replicated for the Enterprise Mobile Support team. They shall have access to the Contractor's Service Desk ticketing platform used for break/fix reports and shall be able to status and resolve tickets generated by the Contractor's Service Desk. They shall also follow existing procedures in using the AirWatch console for MDM related problems. The Contractor's Service Desk Tier 1 agent shall maintain end-to-end ticket tracking, maintaining automated and chat communication with the AT&T Service Desk for MDM, mobile device, and wireless carrier issues. The LCM team shall continue to meet service level responsibilities and shall follow all reports to closure. The following figure illustrates the organization of Service Desk components for mobile users.

County of San Diego Mobile Support Services Methodology


END USER
HPES Service Desk
Create Ticket in Service Portal (SP)
AT&T Enterprise Mobile Support Team
Receive Ticket in SP
AT&T LCM Trade Street Service Desk
Overall Responsibility for Service Assurance on Mobility Reports
AT&T
MSS Application Service Desk
AT&T
LCM Trade Street Service Desk
HPES
Custom App, AD, Email Exchange Group Issues
Applications
Non-Device, Non-HP Apps
Carrier
Non-AT&T Carriers
AT&T
ASD/MSS Service Assurance Team
AT&T
LCM Trade Street Network Engineering
AT&T
ASD/MSS and AirWatch Teams
164 CA CoSD

Contractor shall follow the standardized and documented procedures shown in the table below.

Standard Documented Procedures

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
AirWatch – MDM AT&T Incident	Once ticket is received, or warm transfer of caller from Contractor’s Service Desk after AD password and role has been verified, Tier 1.5 shall work with the End-User to fix the issue. If Tier 1.5 cannot resolve the issue, it shall be given to Tier 2 to be worked through to conclusion. The incident manager shall document in HPE Service Manager, and transfer the ticket to the correct group to fix the issue or resolve the ticket.	AirWatch Console
AirWatch – MDM AT&T IMAR	Once an IMAR is created, IMAR Manager shall review line item and ensure End-User appears in the AirWatch Portal correctly. Monitor to ensure other line items are closed by Contractor and send out instructions to the requester for AirWatch app install and configuration. Working with End-User on deleting the old device when requested. IMAR manager documents change in the IMAR and close.	AirWatch Console

Remote device management

Remote Desktop Management (RDM)

Contractor shall provide a “warm” transfer escalation process between Service Desk and RDM. If support requests cannot be resolved expeditiously by the Service Desk, then the call shall be escalated to an agent with higher level skills and RDM capability. In some cases, the Service Desk agent shall escalate to a higher tier deskside/field team or technical support. Service desk training and detailed documentation outlining the correct escalation path for each type of incident or service request shall guide agents to make certain that tickets requiring escalation are routed correctly the first time. Contractor shall always ask permission from the End-User before accessing his/her desktop, and the End-User can terminate the remote session at any time.

Remote Desktop Management (RDM). The primary function of the RDM agent shall be to provide a higher level of technical service, handling problems and issues that the first-tier support was unable to resolve and providing RDM skills to increase first-call resolution and customer satisfaction. Using RDM for remote tool capabilities, agents shall remain on the phone with the customer for longer intervals than Service Desk agents to resolve an incident. RDM agents may interact with network services, software systems engineering, and/or applications group to restore service and/or identify and correct the core problem. This may require assisting in simulation and re-creation of End-User problems and recommending system modifications to reduce End-User problems.

Remote Desktop Management agents shall:

- Take tickets routed to them that require a higher level of technical analysis and work these tickets to resolution or route to the appropriate Tier 2 technical support group
- Handle problems and issues that the Service Desk agent is unable to resolve
- Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct a core problem
- Assist in simulation and re-creation of End-User problems
- Recommend systems modifications to reduce End-User problems
- Use LogMeIn Rescue as Contractor's remote desktop management tool.

2.7.6 County managed mobile devices.

For County-managed mobile devices (e.g., handheld devices, smartphones, tablets, and other County retained mobile assets), the methodology for MDM shall apply. Any device that is "County managed" and outside the scope of RU fixed price support requires T&M support.

Contractor shall mitigate against risks such as device loss, data loss or breach, and exposure to malware by using inherent capabilities of the AirWatch client.

Through AT&T, Contractor shall enable secure, VPN-based interaction with enterprise data using one of two methods. First, the Pulse Secure mobile client shall allow applications to establish an encrypted connection to the enterprise via the same SSL VPN solution used for enterprise computing. Second, the AirWatch solution shall allow applications to be developed to use "per-application VPN."

Contractor shall enable AirWatch managed content and collaboration features, using the AirWatch Secure Content Locker tool. This tool shall allow for direct access, encrypted access to enterprise data, leveraging containerization capabilities to prevent data transfer to external sources. Secure access to web-based services such as SharePoint shall also be enabled.

4.9. Unified Communications Services

4.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide Unified Communications (UC) Services, which shall enable improved collaboration capabilities across each business areas in the County. These UC capabilities shall include O365, Lync/SfB, Mutare Enhanced Voicemail for voicemail to email delivery as well as Avaya's EC500, which extends both internal and external calls to a County End-User's desk and/or a mobile phone provided by the County. UC capabilities shall be delivered to users on their computer, tablet, smartphone, or VoIP handset.

The following table sets forth when Contractor shall provide the specified UC services:

UC Services

AS OF CONTRACT EFFECTIVE DATE	BY THE END OF TRANSITION	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
• Mutare Voicemail to Email with SST • Avaya IP softphone • Avaya Extension to Cellular • Avaya IP soft phone for agents • Avaya Enterprise Directory Integration	• Avaya Communicator for Lync • Avaya Collaboration Services for Outlook/ Browser/ Microsoft Office	• Avaya Communicator SIP mobile client • Avaya Presence Services

Office 365 Components

Through the County-licensed Microsoft Office 365 cloud offering, which includes Lync/ (Skype for Business), users shall have access to instant messaging, presence, web conferencing, video conferencing, desktop sharing, and interactive whiteboards.

Table 1. Specifies when the County shall receive the various components of O365

MODULE OF O365	AS OF CONTRACT EFFECTIVE DATE	BY END OF TRANSITION	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
Lync and/or SfB	Y (Lync)	Partial SfB	Full SfB by 2018
OneDrive	Partial	Partial	Integrated
O365 Office Apps	Y	Continued Y	Continued Y
eMail	N	Y	Continued Y
SharePoint Online	N	N	T&M

Avaya Integration with Lync (Skype for Business)

Contractor shall deploy Avaya Communicator for Lync, which shall allow users to move from limited peer-to-peer audio capabilities into conferencing capabilities hosted within the Avaya Enterprise voice network. As UC services progress, desktop web conferencing capabilities shall become fully interoperable with conventional Cisco teleconferencing platforms.

Other UC capabilities to be implemented include using Avaya Communicator for Lync and collaboration services, which shall contain plug-ins for Outlook, and providing complete call control from the Lync or SfB client with the following key features:

- Click to Call On-Net and Off-Net local and long distance calls, using an End-User's computing device, mobile, or desktop telephone set
- Click to Answer incoming calls from Lync or SfB, using an End-User's computing device, mobile, or desktop telephone set
- Search and Click to Call internal and external County contacts from Outlook email
- Screen pop with contact on incoming calls from Outlook contacts.

Speech to Text (STT) Integration

Contractor shall use the Mutare Enhanced Visual Messaging with STT service. This solution shall transcribe an End-User's new voice mail message into text via email along with a .wav attachment or a secure web link for streaming the message to the County End-User email via SMTP relay.

Mobile Unified Communications

Contractor shall leverage the AirWatch SaaS MDM solution for deployment of UC mobile (e.g. Avaya mobile client, Skype for Business) applications to the County of San Diego mobile application store for corporate owned managed devices, as well as, upon approval, employee owned BYOD devices. Once the UC mobile application has been deployed, whether on a corporate managed device or an employee owned BYOD device, Contractor and AT&T shall provide full support of the application and its connectivity and functionality to the systems that provide these UC capabilities.

Through the integration of the AirWatch Mobile Device Management (MDM) and the Symantec Managed PKI solution for deployment of PKI payload profiles, all corporate managed and BYOD mobile devices and users shall be authenticated prior to accessing UC services or resources. This shall allow for County mobile users to take advantage of the Lync/SfB mobile application, which provides presence, instant messaging, and other capabilities while on the go. Additionally, through Avaya's Communicator for Mobile application, users shall be provided with full enterprise telephony functionality from their mobile device, allowing them to make, receive, transfer, and put calls on hold as well as use advanced features such as Active Directory (AD) lookups and presence status from Avaya voice and SfB users. Users shall have Full Call Control in addition to common enterprise voice features, such as:

- Make/receive calls
- Hold/retrieve calls
- Transfer calls
- Multiparty conference calls.

UC Data Sharing

UC data sharing shall also evolve from traditional SharePoint and network file share capabilities to enterprise file sharing and synchronization.

- **Email** – This shall be provided by Contractor for all County employees and shall be migrated to Office 365 Exchange Online during the transition phase of the Agreement.
- **SMS** – Contractor shall provide this feature as part of the mobile device services, and this feature may be provided by the carrier of choice by business unit. This shall be a hosted service and shall be isolated to the business unit and not available to the enterprise.
- **Fax** – Contractor shall provide Local and premise-based fax services either through the Avaya PBX or separate 1 MB lines by AT&T Core, and shall ensure that all are supported by AT&T life cycle management (LCM). Additional fax capabilities shall be offered by Contractor via the Right Fax solution, which shall be integrated with Office 365 Exchange Online. This solution shall provide users with fax to email services.

UC Support

Contractor shall provide front line support as a part of both Contractor's Service Desk Services and End-User Services. Support and training resources shall also be provided through the Service Portal. Contractor shall continue to leverage Contractor's previous Service Desk activities as well as develop, update, and maintain Service Desk scripts and processes for the UC End-User community. Contractor shall post training videos. As with all Contractor's Service Desk activities, Contractor's UC support shall include incident tracking, escalation, and resolution.

Teleworker and Remote User UC

Contractor shall deploy, after County approval, Avaya Communicator integrated UC and voice services clients. These integrated clients shall provide the 2,600+ users, and any future SSL VPN County users, access to a complete, consistent, and rich set of capabilities both on-net and off-net. Avaya Communicator desktop and mobile clients shall be able to operate in both VPN and non-VPN mode to provide remote connectivity. Avaya's Session Border Controller, in conjunction with Client Enablement Services, shall allow users of Avaya communicator clients (desktop or mobile) to operate in SIP (session initiation protocol) mode. Enterprise security standards, such as TLS and SRTP (secure real-time transport protocol) encryption, shall provide effortless access to UC and voice services integration, enabling teleworkers to function as if they are in the office regardless of their location.

Software and Release Management

Contractor's subject matter experts (SMEs) shall subscribe to Avaya's UC integrated client updates, service packages, or version upgrades. These shall be thoroughly reviewed by SMEs for County environment relevancy and tested in a lab environment before production deployment is recommended. This standardized process shall validate production functionality of any recommended new release update, service package, or version upgrade so that the County End-User environment is not disrupted or compromised.

Contractor SMEs shall apply industry standard software release management methodologies to support standard version delivery and consistency across all County users' devices and assets. These standards shall apply to Avaya One X Communicator, Avaya Communicator for Lync/SfB, Avaya Communicator Mobile, Avaya One X Agent, and Avaya Collaboration Services. The same shall apply to any proposed applications that need to be deployed to the County's managed mobile devices via the AirWatch MDM solution.

Contractor shall create, post, and document consistent UC client software packages for all client types.

This process shall integrate with all ITSM processes in place to ensure communication, approval, etc. and full integration with the overall program.

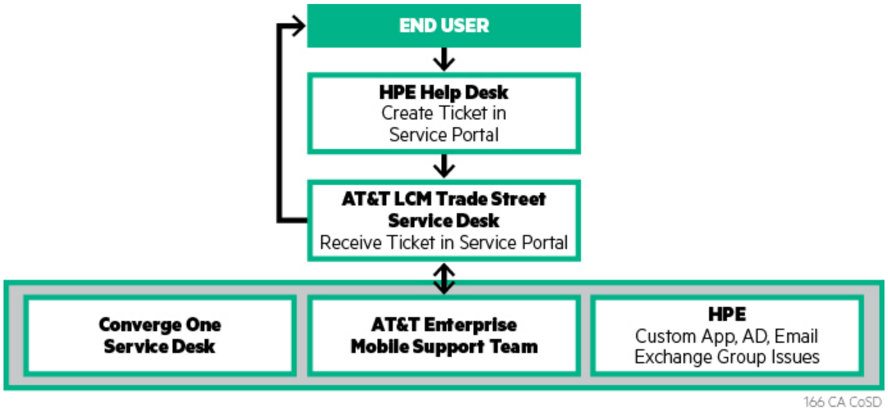
- Deployment plan for resources and use of facilities

As with other services, the County shall use Contractor's Service Desk to support UC. Contractor shall have high-tier support with both AT&T and Microsoft. Contractor's Service Desk shall still own support tickets through the entire life cycle for the convenience of the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

All support services, whether triage, new requests, change requests, or removals shall be initiated by the County End-User to the Contractor Service Desk. All requests that are within the network framework for real/non-real time services shall be directed to the AT&T LCM team for assessment and completion. The following figure illustrates Contractor's support services methodology.

County of San Diego Unified Communications Support Services Methodology


END USER
HPE Help Desk
Create Ticket in Service Portal
AT&T LCM Trade Street Service Desk
Receive Ticket in Service Portal
Converge One Service Desk
AT&T Enterprise Mobile Support Team
HPE
Custom App, AD, Email Exchange Group Issues
166 CA CoSD

The following table delineates services Contractor shall perform for End-Users in accordance with the standardized and documented procedures.

Services to be Performed by Contractor for End-Users

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
Mutare EVM Incident Request	Documented process for End-User request to repair trouble with Mutare EVM service	Service Center
Mutare EVM IMAR Request	Documented process for End-User request for active or new service for Mutare EVM	Service Center
Avaya IP Softphone Incident Request	Documented process for End-User request to repair trouble with Avaya IP Softphone service	Service Manager
Avaya IP Softphone IMAR Request	Documented process for End-User request for active or new service for Avaya IP Softphone	Service Manager
Avaya Extension to Cellular Incident Request	Documented process for End-User request to repair trouble with Avaya Extension to Cellular service	Service Manager
Avaya Extension to Cellular IMAR Request	Documented process for End-User request for active or new service for Avaya Extension to Cellular	Service Manager
Avaya IP Softphone for Agent Incident Request	Documented process for End-User request to repair trouble with Avaya IP Softphone for agent service	Service Manager
Avaya IP Softphone for Agent IMAR Request	Documented process for End-User request for active or new service for Avaya IP Softphone for agent service	Service Manager

For quality UC support, Contractor's SMEs shall use numerous automated tools. These tools shall enable Contractor to continuously monitor the overall health and performance of voice appliances, assist in rapid restoration through fault isolation, and perform traffic analysis as shown in the table and discussed further below.

Contractor shall deliver complete manufacturer system maintenance coverage on all County Core Voice Services assets. Together, these tools shall provide complete health monitoring and expeditious issue resolution. Avaya Expert Systems and Secure Access Link shall be online and engaged 24x7 to diagnose and attempt to resolve known system alarms, clear many service affecting issues, and escalate to engineering resources for prompt attention when necessary.

Contractor's UC team shall use Nectar's UCMP and its complete suite of innovative features to provide the County enhanced, integrated network services. Nectar shall provide multivendor management services including application dependency tree visual alerting and vendor knowledge modules, which shall help Contractor's SMEs proactively pinpoint and resolve cross-platform integration issues quickly and restore services to County users. The UCMP shall also include real-time network quality of service reporting using RTCP integration, and shall be able to create simulated traffic injection between designated network segments for analysis. This shall allow the SMEs to monitor and report on all VoIP related traffic transmissions.

The quality of service reporting tool shall provide per-hop statistics and in many cases shall assist in quickly identifying improper packet handling hop points. The Nectar platform shall include statistical resource utilization data gathering and storage that shall enable trending analysis and capacity planning. These capabilities shall be available using an intuitive and customizable dashboard with visual and electronic alerting from sophisticated threshold configurations. The dashboard shall allow Contractor to acknowledge, respond, and correct issues proactively, in many cases before County users know or report an issue.

4.10. Catalog Services

4.10.1. Process and Procedures

- Description of solution to meet the requirements

Solution Summary. The Optional Item Catalog (OIC) shall hold all approved single user applications, standard and nonstandard hardware items, and support only services.

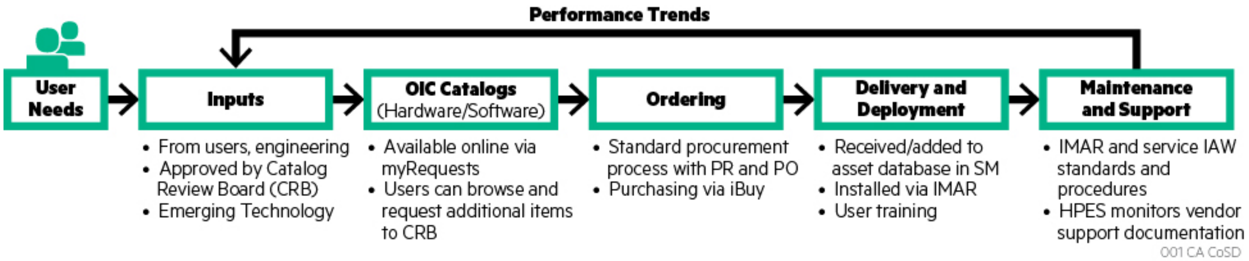
The configuration of the catalog shall be controlled by the Catalog Review Board (CRB). The board shall consist of Contractor and County selected points of contact (POCs) from each department to discuss, review, and approve items for inclusion in or removal from the catalog.

Catalog activities, such as ordering, maintenance, and approval, shall be accessible online via the Service Portal and myRequests. While all users shall be able to order, only select users shall be able to perform other functions––review and approve, for instance—based on their organizational role and authority. myRequests shall be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in the Transition Services Framework.

Requirements and requests for new catalog items or updates can come from users, engineering analysis, new technology offerings from HPE, third-party vendors, and elsewhere. County desktop hardware peripherals, laptop accessories, stand-alone printers, and desktop software prices shall be reviewed on a quarterly basis by HPE Global Procurement through a Request for Quote (RFQ). Contractor shall check with suppliers to compare prices and delivery schedules to match the existing catalog and make the necessary changes. Once the catalog manager receives the updated list from HPE Global Procurement, he/she shall update the OIC. The updated list shall be reflected in the following OIC publication, which shall occur on the 20th of every month. The catalog shall be updated with new End-User hardware peripherals and End-User software, including pricing on these items, one for hardware replacement and one for end of life (EOL) hardware.

The figure below provides a summary of the OIC solution—rom identification of item need to delivery and support.

The OIC Process


Performance Trends
User Needs
Inputs
OIC Catalogs (Hardware/Software)
Ordering
Delivery and Deployment
Maintenance and Support
• From users, engineering
• Approved by Catalog Review Board (CRB)
• Emerging Technology
• Available online via myRequests
• Users can browse and request additional items to CRB
• Standard procurement process with PR and PO
• Purchasing via iBuy
• Received/added to asset database in SM
• Installed via IMAR
• User training
• IMAR and service IAW standards and procedures
• HPES monitors vendor support documentation
001 CA CoSD

Once approved, the catalogs shall be available via the Service Portal. Users shall order via myRequests using functionality described in the “MyRequests User Guide.”

For nonstandard items that are already installed and deployed, Contractor shall support OIC items through the warranty period for hardware. If additional assistance is needed, Contractor shall implement other processes to provide support for these items.

User training shall be available on OIC items, as necessary. OIC items shall be monitored by Contractor for manufacturer updates and shall be incrementally refreshed as recommended and approved. Specialized End-User support for applications shall depend on the nature of the applications and the problem. Technical and configuration support shall come from Contractor’s break/fix technicians. If the issue is determined to be related to an application with a Portfolio Application Identifier (PAID), identifying it as a supported application, Contractor’s Service Delivery Manager (SDM) for the business unit shall work with the vendor and the County apps owner for that portfolio application.

Each item in the hardware and software OIC catalogs shall be sorted by category, with a brief description, manufacturer, model/reference, and a unit price. For commercial items, pricing shall be set competitively via Contractor’s procurement organization in agreement with the RFP requirements. If an End-User selects an item that requires End-User Service support for installation, those requests shall be added at the end of the optional item ordering process.

On the software side, there shall be three categories of desktop software:

- Purchase - Software products that are available for purchase.
- Supported but no longer available for purchase – Software products that are part of the Desktop Application Directory but are no longer available for purchase (for example, old versions of software). These products are still supported by Contractor.
- Other desktop software - Software that can be installed if licensing is in place. An analyst contacts the requester to discuss licensing before the software is installed.

- Deployment plan for resources and use of facilities

The OIC shall be available via the Service Portal in myRequests, both of which shall reside on servers at the Contractor data center. OIC management and deployment/service of optional items shall involve Contractor resources in management, engineering, procurement, and End-User services, most of whom shall be assigned to the Rancho Bernardo site. Others shall be part of a virtual team from across the U.S.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Online Catalog. The OIC shall list items available for purchase by County users and shall contain standard items as well as optional items. Users shall be able to shop for items available for one-time purchase or RUs (monthly fee), including bundled services. Users shall also be able to suggest changes to the catalog. When an item is approved and an order is placed, Contractor shall fill the order and deliver the products to the requester. Contractor shall:

- Coordinate an installation appointment with requestor
- Assist with set-up, including physical installation and connection of the device to the workstation or network
- Assist with the initial loading of the software products listed in the catalog,

The OIC is accessed from the myRequests page, which shall reside as a link from the Service Portal.

Viewing/Modifying Catalog Requests

All catalog requests shall be viewable by the requestor but shall only be able to be modified prior to submission. If a change is needed after submission, the End-User shall need to clone the request, make the changes, and delete the old request. The End-User shall be able to see the purchased status of an item by clicking the Purchasing tab.

Reviewing and Authorizing Catalog requests. If an End-User is a reviewer for the Catalog, they shall be able to access requests that have been submitted. These requests shall appear on the Review Catalog Requests screen. After accessing a request, the reviewer shall make comments that are then sent back to the requestor, rejecting or approving the request as submitted.

Shopping from the Catalog

An End-User shall be able to order hardware, software, or services from the catalog including video conferencing equipment, audio-video equipment, and telephones, computer and phone services, or special bundles for new employees. For all catalog orders that involve site installations, they must be authorized by the County Technology Office, who shall be notified by the myRequests system.

Billing, Authorizer, and POETA

After a request is made, the End-User shall be prompted to enter their billing and authorization information. myRequests shall use this information to "file" the request with the appropriate County agency and provide the correct financial account management. Each letter in the word "POETA" stands for a different billing item. The End-User can contact the financial coordinator of the business group for the correct information to submit. Billing shall be in accordance with the supplied POETA information.

Procedures. Catalog updates shall be managed in coordination with other standards governance activities, including the annual standard desktop configuration update and the weekly architecture review meeting. The catalog shall be updated in synch with other configuration changes.

The key to continual improvement in the Catalog Services component shall be to perform benchmarking with vendors, making sure that the catalog is refreshed regularly, is responsive to End-User needs, and that catalog optional items integrate and interoperate well with the standardized core configurations. Each new component shall be SIT and UAT tested and approved by the County.

4.11. Network Printer Services

4.11.1. Process and Procedures

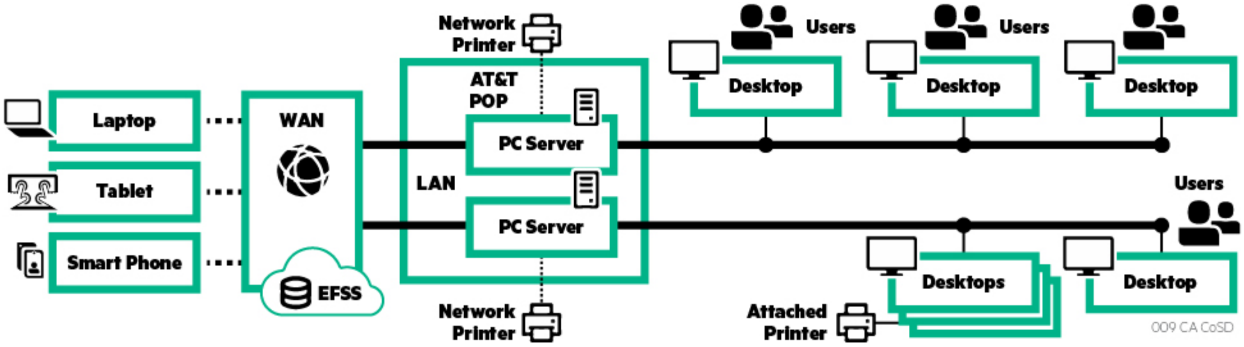
- Description of solution to meet the requirements

Network printers shall be integrated into the End-User service model and network architecture seamlessly.

The network printer support solution shall be the same for all types of printers. The only difference shall be in configuration and utilization information related to specific makes and models of printers. The figure below summarizes the network printer configuration.

Network printers shall be standardized attached devices and are operated and maintained under many of the same procedures for hardware and core software. Desktop services shall handle the printers, their configurations, drivers, and the queues. The local server team shall manage the print servers located in the AT&T POP and in the DR POP location in San Diego, as well as other locations where servers are installed throughout the County (such as FRCs and CAC).

Network Printer Architecture



- Deployment plan for resources and use of facilities

Contractor shall perform this work from Contractor's Rancho Bernardo site.

All service technicians shall have basic training and skills in network printer operations, maintenance, and troubleshooting. Contractor shall have a hardware team that specializes in printer/server support, but all field technicians shall be trained at a basic level to support these devices. Printer specialists shall be embedded in the Desktop Services organization but shall not be a separate team.

Contractor's technicians shall have the same core skills but different levels of expertise in specialized areas, such as surge and DR situations. Because of this, Contractor shall be able to cross-assign staff to a critical area.

- Key methodologies and processes in solution including year-to-year continuous improvement

Printers are a specialized device on the network, but the overall processes and procedures described previously in the End-User framework shall apply to printers. Printer management shall involve printer specific activities such as:

- Printer service IMAR and operations
- Printer device management
- Queue setup
- Load balancing
- Printer security management
- Configuration setup and management for groups and individual users.

The requirements to support network printers shall be part of Contractor's plan, build, operate approach. The table below maps each of the framework component requirements into a Plan, Build, and Operate (PBO) phase and then summarizes Contractor's solution and methodology and key processes.

Mapping of Framework Component Requirements for PBO Phase

STAGE	COMPONENT REQUIREMENT (SUMMARY)	CONTRACTOR'S SOLUTION, METHODOLOGY, AND KEY PROCESSES
Plan	Standardize	• Printers are included in annual engineering and standardization reviews • The County approves standard printers
Plan, Build, Operate	Provide back-end infrastructure	• Printers must be compatible with the County Architecture • Network capacity is engineered to support printers
Plan, Build, Operate	Upon device failure or network failure build in redundancy and failover procedures	• Engineer and maintain for reliability and recovery
Operate	Keep drivers current; maintain firmware (slightly specialized)	• Drivers are maintained via SCCM • Firmware versions are monitored via vendor FAQs and pushes
Plan, Build, Operate	Categorize printers; printers are either standard resource units or in the OIC	• Several classes (monochrome, color, high performance, large format, label and multifunction devices) of network printers are installed • Printers are in Report 44 and the OIC
Build and Operate	Support the User – develop training, tip sheets, update the portal, among others	• User support materials are built by engineering once the printer is selected
Build and Operate	Continuously maintain Service Desk scripts and support info for technicians	• Printer install and End-User support materials are built by engineering • Tickets feedback inputs to improvements
Plan, Build, Operate	Leverage existing licenses	• Printer timeline and refresh strategy is maintained to reduce cost of licenses • Strategic negotiation and leverage utilized for license costs
Plan	Make effective standards at the start of each new year	• Printer standards are selected as part of the annual standardization process • Printer vendors brief County and Contractor on current products and migration path(s)
Plan and Operate	Supply via the portal a list of consumables	• Consumables list to refreshed annually along with the standards selections • The County can therefore forecast consumables expense and do supply management
Operate	Excluded printers not attached	• Concur
Operate	County shall be responsible for consumables	• Concur

STAGE	COMPONENT REQUIREMENT (SUMMARY)	CONTRACTOR'S SOLUTION, METHODOLOGY, AND KEY PROCESSES
Operate	Maintenance, availability, and break-fix	• In agreement with overall service and break/fix methods • Printer experts are available to assist at all Tiers of support
Plan	Maintain and update annually a timeline/roadmap regarding support to active devices and planned tech refresh	• Printers are part of the overall standards assessment, engineering, test and governance The County approves the standard printers and any OIC printers

4.12. [Reserved]

5. NETWORK SERVICES

5.1.1. Process and Procedures

Bandwidth and capacity management and reporting.

Contractor has tailored its bandwidth and capacity management processes to meet the County's increasing needs. Bandwidth shall be proactively delivered to County locations before link saturation affects performance. This process shall begin with weekly reporting on key capacity metrics using AT&T's CA spectrum and eHealth tools. These tools trend bandwidth and latency against baselines. These trends shall be validated as legitimate business traffic using AT&T's deep packet analysis tools before action is taken. Using the thresholds below, which may be modified by mutual agreement of the parties, Contractor's Capacity and Performance Monitoring team shall make recommendations for bandwidth upgrade in the weekly Operations Governance. This approach to capacity management helps the County of San Diego provide the right level of capacity at the right location and at the right time.

Below are the thresholds for both WAN and Internet Transport:

Bandwidth Utilization Threshold (WAN): 90% Peak Utilization over 4-week period of time + corresponding latency threshold breach
Bandwidth Utilization Threshold (ISP): 90% Peak Utilization over 4-week period of time + a 1.5 – 2Mbps drop rate
Latency (WAN): GigaMAN (greater than 4ms), Opt-E-MAN/NoD (greater than 8 ms), T1 (greater than 15 ms)

As part of this process, Contractor shall provide:

- Weekly review of network capacity metrics as part of the County's operational governance process.
- Capacity management that meets the business needs of the County using tools that provide real-time threshold alarming.
- Communication of findings and recommendations that help the County achieve optimal utilization and capacity.

The local team shall continue to meet weekly with the County's operational team to present and review findings and make recommendations. Contractor shall perform optimization analysis daily using its automated tools that aggregate findings and establish trends that become the basis of Contractor's weekly reporting.

Contractor shall migrate remote sites to AT&T's Switched Ethernet (ASE) with Network on Demand. This allows the bandwidth and capacity management practices for the County to become even more dynamic. Using the software-defined networking capabilities that are inherent to ASE with/Network on Demand, bandwidth can be adjusted from as low as 2 Mbps to as high as 1 Gbps in 15 minutes.

Contractor shall implement a solution whereby adjustments can be made within the Network on Demand infrastructure on a scheduled basis, providing the County a great deal of flexibility in bandwidth management. As an example, if the County Health and Human Services Agency planned an employee training event that required heavy video and interactive content (not distributed using a centralized, multicast town hall solution), Contractor's capacity team schedules an adjustment to specified remote sites for an agreed period of time. This shall deliver the required bandwidth where needed and, at the completion of the training, automatically adjust the bandwidth back to its normal business capacity.

Real-time bandwidth adjustments shall also be made as needed. This may be required as the result of unexpected local or national events creating unanticipated demand on the data network. As future events occur, Contractor shall be able to do more than just increase the ISP bandwidth. By using its capacity and performance monitoring tools, Contractor shall analyze the traffic and determine if it is affecting the County's WAN. At that point, real-time adjustments shall be made to alleviate the congestion in minutes.

All transport services—including WAN, AVPN/MPLS, ISP, and SIP trunking shall be scaled to maximum interface capacity as well as built in parallel so that growing County bandwidth needs are met over the life of the term. Also, as new services are made available with additional speed or throughput capabilities, Contractor shall require AT&T to evaluate the feasibility of such services and make corresponding upgrades where reasonable under existing service commitments.

Performance monitoring and reporting

Contractor shall provide the data necessary to optimize network service to the County. Capacity planning is used to determine the network resources necessary to prevent performance issues from impacting these critical network services. Performance monitoring/management is the process of managing network and data services response times, consistency, and overall service quality.

Contractor's network team shall administer, monitor, maintain, and manage performance of the data network services and network services infrastructure. This shall involve input from many areas of the business to identify what IT infrastructure is required to support the County's business.

The process components shall include:

- Performance monitoring for routers, switches, firewalls, and network servers and appliances
- Capacity monitoring of WAN transport circuits
- Internet performance monitoring of public and staff CIR
- Trend reporting and analysis.

Key sub-processes shall be:

- Network bandwidth monitoring to specified thresholds
- CPU/memory utilization and errors monitoring on all network devices to specified thresholds
- Responsive impact assessment and mitigation planning
- Proactive trend-based "situational watch list" assessments and corresponding action plans
- Real-time traffic analysis initiated from "exceeded threshold criteria" in the form of Spectrum critical alarms.

Performance Monitoring Tools

Using AT&T's capacity and performance management functions that utilize various toolsets, Contractor shall provide monitoring, reporting, trending, and analysis services to the County.

CA's eHealth and Spectrum tools shall integrate to maintain critical service levels across complex network environments by combining eHealth's automated availability and performance management with the Spectrum network service and analysis platform.

The eHealth and Spectrum tools shall allow for more efficient alarming and reporting, enabling the network capacity and performance management team to focus on proactive troubleshooting, performance optimization, and service level management.

Another toolset that shall help manage system performance within the County network infrastructure is Riverbed Cascade Profiler, which provides a unified end-to-end view of service delivery, application, and consumption from the data center to the End-User. Cascade Profiler assists in troubleshooting the threshold deviations reported in eHealth, troubleshooting in real-time and from a single probe interface. Cascade retrieves real-time information, providing quick and easy access to logical views such as link analysis, link usage over time, Top N applications, and Top N conversations and hosts.

Troubleshooting and Forensics

The above mentioned promiscuous tools enable event correlation and forensics through the active capture of network traffic combined with reporting capabilities that provide real time and historical data. This capability applies not only to the previously mentioned tools, but also includes the deployment of desktop based tools such as Wireshark, which are used as needed to conduct packet captures from individual assets. When used in active troubleshooting, all of these tools are used to correlate the event to a root cause for resolution by the appropriate framework using cross framework troubleshooting processes.

Performance Baselines

Contractor shall use these tools to provide data on specific metrics for historical and baseline performance evaluation. These baselines are important in Contractor's monitoring of the County's network since they can directly affect bandwidth provisioning and other resources.

Performance Threshold Alarming

Once baselines have been determined, thresholds shall then be established based on variables within the network infrastructure. Circuit measurements depend on bandwidth to determine baselines and thresholds. Physical devices such as routers and switches report memory allocation errors, CPU utilization, and buffer hits. There are also broader ranges of environmental specifications to which thresholds are tracked, such as power supply, fans, and temperature, among others.

Threshold severity is currently defined in four levels, each dictating an appropriate course of action as listed in the table below.

Threshold Severity

SEVERITY	ACTION
Warning	Track element status on weekly basis.
Minor	Add to Watch List (document in Situation-to-Watch and status any changes).
Major	Assess and engage relevant framework, open internal ticket if necessary. Add to Watch List.
Critical	Trigger to "Attention" notification tool, initiate internal break-fix. Troubleshoot and actively mitigate until resolution.

Critical alarms shall be sent to the Attention application system that notifies the NOC operations team (and on-call) members via phone, SMS, and email. The Attention system software shall provide a predefined notification process for critical alarms as well as escalation processes for overdue or pending alarms on a 24x7 basis.

Other important thresholds that have been established include site latency and Internet CIR thresholds. Site latency thresholds shall include latency deviation based on the type of circuit. Internet CIR thresholds shall be triggered when bandwidth use on the Internet link goes 20% above the daily average, as measured by eHealth and in conjunction with quality of service (QoS) policies applied to the Internet router.

Performance Trending and Analysis

Once baselines and thresholds have been established, Contractor shall perform trending and analysis. There are a number of variables that contribute to the analysis of a trending element. Bandwidth use, CPU use, physical hardware errors and application response time delays can all have an impact on network health. eHealth reporting (Situations-to-Watch, Top N Reports defining baseline statistics, Health Index Reports indicating CPU, errors, and discards) along with Cascade Profiler reporting (application response time statistics, link usage, top application layer applications and hosts) shall be used to collectively qualify and pinpoint performance degradation associated with the network or an application. This detailed information shall drive necessary corrective actions as well as engagement of the appropriate Contractor framework in problem resolution.

Reports showing an increase in trending for elements in the network shall be reviewed and investigated for further analysis. Report trending from Situations-to-Watch, Top N latency, and health index reports shall be addressed by further analysis with a deeper dive into the affected element(s).

Adjustments made to correct issues associated with variables related to bandwidth use, memory allocation errors, CPU processors, or other changes in the network, shall be based on investigation of the specific cause. Increasing the bandwidth for a specific County site shall be determined by identifying historical data and trending analysis for a specified period of time. There shall be an initial assessment and continued monitoring of the network thresholds (application, End-User count, throughput and other associated activities) to validate the appropriate remedy for a given issue.

Real-Time Anomaly Detection

As the Contractor Operations team begins developing processes around real-time anomaly detection, they shall develop automated alarming and event correlation capabilities, with focus on application performance. The tools mentioned in this section—along with other data center and desktop-based platforms—shall enable a layered approach to event triangulation, which, combined with the daily stand-ups, improves the proactive performance management of services across the enterprise. Contractor shall dedicate resources to improving proactivity over the life of the term, with measured results reported through the operations governance process.

Data Aggregation and Analytics

Contractor shall contribute key capacity and performance tool data to the cross functional data warehouse, with focus on bringing enabling automation and continuous improvement through a global analytics and reporting practice.

Contractor shall work with the County in extending both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured as follows:

- Service Strategy and Improvement Analytics: This area focuses on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis
- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.
- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, Contractor can conduct analysis to reduce business impact of events, incidents, and problems.
- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Performance Reporting

Contractor shall ensure that tools are in place, baselines and thresholds are completed, and trending and analysis processes are established to provide reports to the County that affect not only bandwidth provisioning, but adjustment and potential corrective action to a wide variety of County resources. On-demand reporting shall be available upon County's request for fast turnaround on critical and time sensitive issues.

Trend and health reports shall be scheduled monthly to collect data and identify the top volume and health index leaders throughout the County network infrastructure. The report shall identify contributors that qualify for threshold conditions such as, use, CPU, memory, errors and latency.

Elements each month shall be sorted by the Top N elements and performance indicators that require attention or resolution. A summary analysis shall be presented for the monthly activity and shall provide watchful situations or those exceeding threshold limits that require corrective actions.

Included in the monthly reports shall be a "Monthly Summarization Report." The details in this document shall include opened tickets for County sites that were affected by latency, bandwidth, errors, CPU, and memory related performance issues.

New and layered approaches to integrating capacity and performance and real-time anomaly detection shall be defined that leverages multiple toolsets. This shall involve cross-framework teams that proactively respond to enterprise issues affecting End-Users.

Identification and Elimination of single point failures in Network Services.

The County increasingly relies on the continuity of the data network for its business functions to remain operational under any circumstance. With this in mind, Contractor shall focus heavily on redundancy and survivability of critical core network services.

Contractor shall avoid single points of failure in its network elements (such as circuits, central offices, and core network elements) via AT&T's redundant network design and software defined infrastructure. These redundancy solutions allow Contractor and AT&T to maintain continuity of the regional, nationwide, and global backbone in the event of isolated failure. One dynamic of the County network solution leverages this redundancy through the use of diverse pathway and ISP exchanges in both San Diego and Gardena, California. With this configuration, the geo-redundant County ISP service remains dynamically available in the event of a regional service interruption.

Increase of visibility into all data communications and data flows between End-Users and Services within the Data Center.

Effective tools are not the problem facing proactive performance management. It is the practice of modeling, trending and analysis that can unlock the potential of the data the tools can deliver, if performed with a broad understanding of the enterprise.

Contractor shall create a cross-framework predictive analytics team whose charter is to manage performance on an enterprise basis. This team shall create and execute a repeatable process to be documented in the Standards and Procedures Manual using a layered approach using numerous tools to monitor and respond to shifts in baseline data.

By developing baseline traffic patterns for network, application, desktop, server, and management traffic, this team shall define thresholds and event patterns, allowing the team to take predictive action, correlating anomalies in the environment. Using the multiple sources of data, Contractor shall conduct daily stand-up calls where threshold breaches are evaluated and diagnosed. This team shall open internal operational tickets on the issues and shall have the authority to escalate across any framework to engage resources as needed to respond and identify the source of the anomaly. Ongoing reports shall be provided to the County operations team and covered in weekly governance meetings, identifying open issues that are being monitored as well as successful closures.

Contractor's County Operation team shall also be tasked on an ongoing basis with improving processes, tuning their practices to better predict, correlate and resolve anomalies. This team shall also have the responsibility to train on their tool sets, improving their mastery in the art of performance analytics. Further, Contractor shall evaluate new and emerging tools that it proposes for implementation, adding to the depth of the data sources at the County's disposal.

The members of this team shall be identified by each framework as responsible for performance management in their discipline and will dedicate the necessary time to maintain a best in class performance analytics function. By taking early action, this team shall drive through chronic issues and eventually reduce the effort for their resolution. Tools and practices, effectively used together, shall increase the visibility of anomalies across the enterprise, improving the End-User experience while maximizing organizational performance and business output.

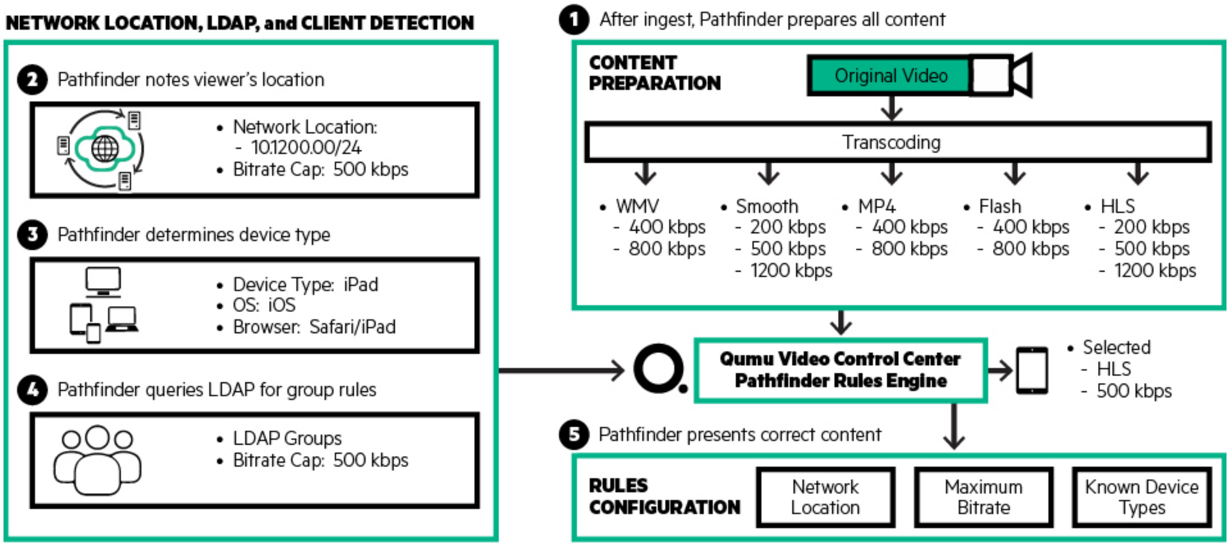
Town Hall Services.

Contractor shall use AT&T Video Management Services (AVMS) and its partner Qumu to provide town hall video services for the County.

Through AVMS, Contractor shall provide all of the functionality needed to capture, manage, and publish video content for both live and video on-demand (VoD) distribution for local and remote users. AVMS's advanced transcoding capabilities shall support formats from various capture devices—from production studio and video conferencing platforms to mobile devices and video cameras. For distribution, the solution shall allow for consumption of video content on a wide variety of devices such as laptops, desktops, tablets, and smartphones while optimizing the End-User experience based on the device being used and bandwidth available.

By means of Pathfinder, AVMS' intelligent routing and distribution element, Contractor shall optimize and present content viewing based on device, network location, and bandwidth, as illustrated in the following figure.

Optimization of Content Viewing



Contractor shall use subdomains to provide separate access to video intended solely for users on the County domain, such as internal communications or training. Internal and mobile video viewing shall have the option to be limited to specific groups based on active directory (AD) group.

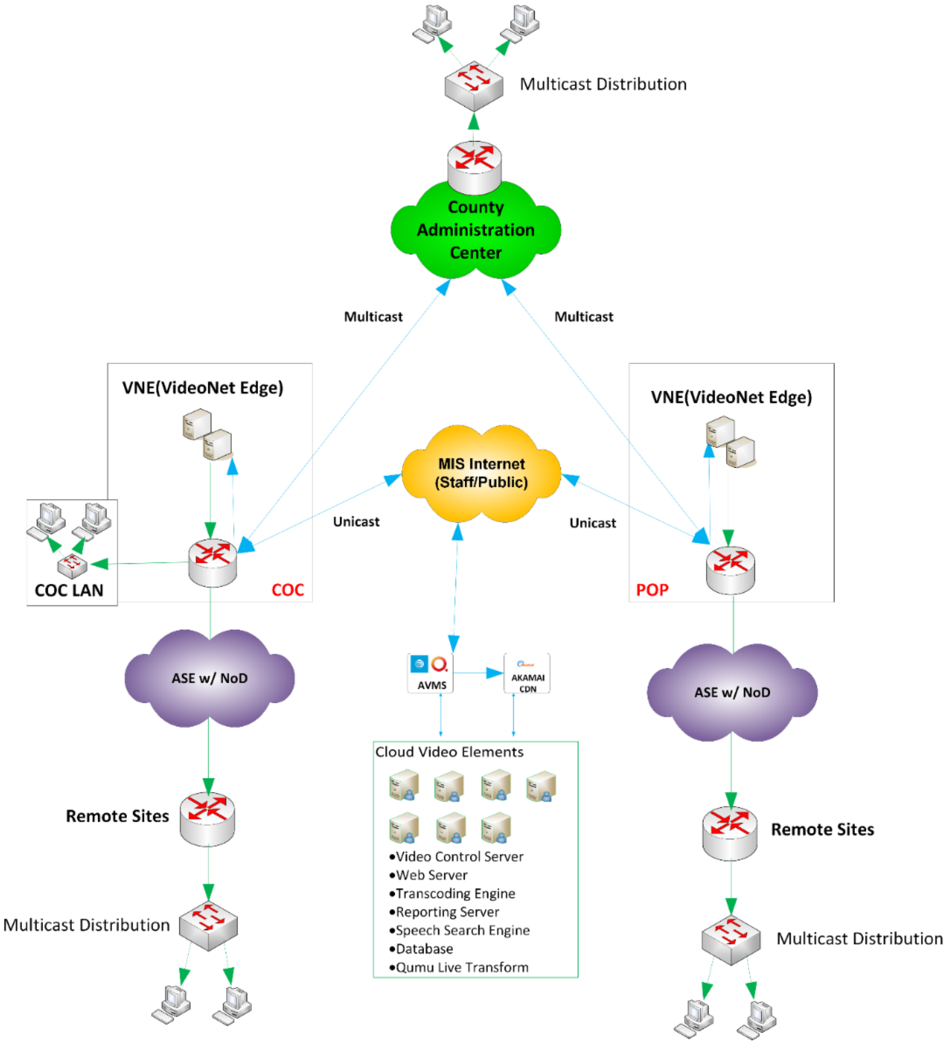
Embedded polling and feedback features shall be included to offer increased benefit to the County by engaging viewers and soliciting their input. Contractor shall use high grade analytics to provide viewer statistics along with broadcast performance detail to provide a clear picture of content performance and identification of possible impacts.

AVMS offers both on-premises and cloud-based options. Contractor shall use the cloud-based architecture, which provides high availability without the need for extensive local hardware and associated support costs. With the added benefit of burst capacity for mobile or public users in real-time, the solution is able to handle traffic spikes without degradation of the delivery quality. The hosted solution can scale to cover all of the County users with growth up to 100,000 simultaneous viewers. With archiving capabilities, video content can be preserved and made available for replay for a configurable length of time.

AVMS makes use of both internal and external Content Delivery Network (CDN) technology. For external content delivery, Contractor shall leverage the Akamai platform. This external content delivery shall be used to augment or replace the Granicus streaming solution.

From within the County domain, the AVMS solution shall enable multicast video presentation through VNE’s (VideoNet edge) to multiple viewers simultaneously without causing an exponential impact to network performance. Contractor shall implement four VNEs, two at COC and two at POP. From this geo-redundant core, the multicast stream can be routed across the WAN to the remote edge, where the LAN redistributes the stream to each requesting End-User.

AVMS Topology



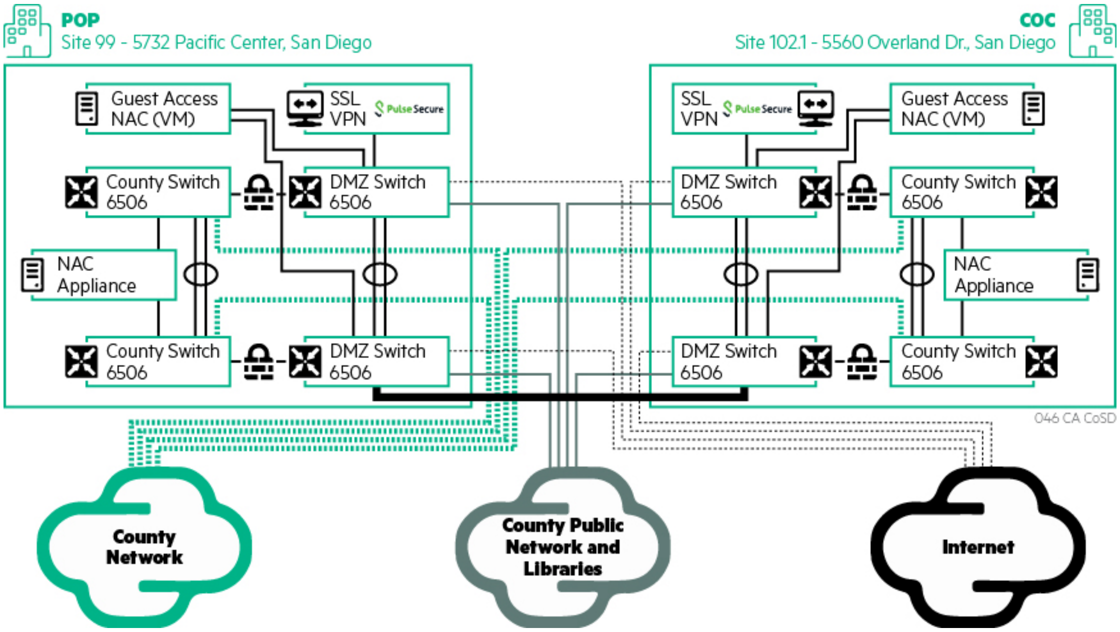
Topology of the AVMS solution, highlighting cloud based services feeding geo-redundant Video Network Edge devices that feed multicast video streams to the remote County sites.

In order to represent a complete solution with no limitations to the County, Contractor is only Providing AVMS for enterprise video content distribution. Contractor shall implement this service within one year of County approval. The solution shall be charged through a fixed monthly Resource Unit Fee for an unlimited number of townhall events. Such RU Fee may be allocated to business units based upon the County’s discretion.

Network access controls and PKI-based device authentication for Wireless Services.

Contractor shall use Aruba’s Clear Pass Policy Manager (CPPM) to provide a comprehensive yet integrated NAC solution. This product shall provide the County all the features of NAC in a single platform to ease management, administration, and troubleshooting efforts. Contractor shall use an integrated RADIUS server, coupled with the ability to perform guest access authentication, shall provide a wireless solution enabling County staff and the public appropriate, policy based network access across any access point in the County. This solution shall provide a seamless authentication for the staff while allowing various options for the redirection of public or untrusted devices. While the wireless deployment is planned to be implemented first, the solution shall function on all physical ports Countywide.

NAC/Guest Access



NAC/Guest Access centralized management topology is provided via a geo-redundant architecture.

The Aruba NAC solution shall be implemented to align with Contractor's geo-redundant, high availability standard. One appliance shall be located at the AT&T POP and one installed at the County Operations Center (COC). These appliances shall manage and enforce policy on the staff wired and wireless infrastructure by leveraging 802.1X and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

The solution shall allow any County domain joined device that is plugged into the network, and logged into with a valid active directory account, to be given access to County network resources. Any devices plugged into the wired network that do not meet the above criteria, or predefined NAC policies for non-domain joined or non-dot1x compliant devices, shall be placed onto a public VLAN with restrictions that allow for access to the Internet only.

The integration with the existing wireless infrastructure shall continue to leverage EAP-TLS to validate certificates for access to the existing County secure wireless network. The certificate required to authenticate, as well as the wireless profile, shall be installed at the time a computing device is prepared for distribution by means of a group policy object (GPO) push within the desktop framework. This GPO is the only way the client machines can receive the certificate required.

To provide public guest access, the Contractor shall install a virtual instance of a clear pass policy manager in the DMZ at both the AT&T POP and the COC for redundancy and resiliency. This provides guest access on the public Wired/Wi-Fi network. The solution shall force all users of the public network to view the captive portal splash page where terms and conditions can be presented and must be accepted prior to being granted access to the Internet. The contents of the splash page, as well as the look and feel (theme), can be modified to include desired content or photos and provide automatic forwarding, after acceptance of terms and conditions, to the County's home page.

The guest access solution shall also offer functionality that shall be leveraged for business unit specific use cases.

Contractor shall maintain a RADIUS server (steel belted radius [SBR]) that acts to authenticate radius sessions from the wireless network. The Contractor team shall leverage the two Aruba appliances planned to be installed at the AT&T POP and the COC to provide radius server functionality in place of the existing SBR server. The two appliances shall be fully redundant, thereby removing a single point of failure and providing all services currently offered by SBR. Contractor shall integrate the new radius servers with the Microsoft CA infrastructure, as well as the new Symantec-managed PKI solution.

Generally, staff users are unaware of any additional security when using a managed County computing asset. The EAP (Extensible Authentication Protocol) required to validate the End-User and machine shall leverage currently logged-in End-User credentials and domain membership to allow access.

Transformation Opportunities

Currently, the County is evaluating cloud-based services to provide cost-effective ways of delivering services to employees and constituents. Contractor's team has already identified the transformations required to receive the full benefits of cloud architecture. Contractor is proposing an AT&T NetBond solution that extends connectivity using a Multiprotocol Label Switching (MPLS) network into County-selected third-party vendors. The NetBond solution provides a secure, performance-assured interface to the cloud, while offloading the Internet Service Providers (ISPs) and dedicating bandwidth to the services. Additionally, Contractor's proposed solution facilitates fully integrated and centralized connection management functionality and supports third-party cloud services with Contractor's contractual service levels.

The foundation of this service is to be deployed in a geo-redundant manner, using AT&T Virtual Private Network (AVPN) MPLS circuits; it is included in the Data Network Services and is priced. Future implementations of NetBond services (proposed as a resource unit (RU) on a bandwidth basis) use this transport connectivity to create the peer-to-peer connection with the selected cloud provider (cloud provider costs may apply).

In support of the transition of Exchange to the O365 cloud, and in line with Microsoft's recommendation, Contractor shall ensure adequate bandwidth is provisioned on the geo-redundant Internet ISP's to allow access to O365 services. As an option for isolating this service away from the ISP, Contractor shall also offer optional NetBond functionality in a peering arrangement with Microsoft's Azure Express Route product. The solution shall be evaluated as a part of the design effort and shall be offered as an optional service, and priced as a separate RU that combines the NetBond RU with the Express Route costs to complete the connectivity model for the service.

5.5. Data Network Services

5.5.1. Process and Procedures

Collaborative Approach

Through involvement in weekly CTO architecture sessions, as well as participation with the Enterprise Architecture (EA) governance process, Contractor shall propose new technologies that have been evaluated and measured against County strategy and business requirements. This continual dialogue with the County, along with Contractor's broad industry knowledge of network solutions and their impact on adjacent technical disciplines, allows the Contractor team to successfully propose and implement emerging technologies within or even before the agreed-upon technology refresh cycles. This approach allows the County to quickly realize the benefits of new technologies. This ongoing interaction also facilitates the standardization of hardware and software deployed by the Contractor team as its solutions receive initial approval from the Enterprise Architecture Forum and subsequently from the Change Review Control Board prior to transformation.

Upon activation of its approved solutions, Contractor shall employ several automated tools to maintain an accurate and up-to-date inventory of all hardware and software supporting data network services. In addition, Contractor shall use automated tools to continuously monitor the provisioned services from an operational and bandwidth utilization perspective, as well as provide valuable insights into traffic patterns and application functionality.

Monitoring and Management Approach

From an operational view, Contractor's capacity and performance management tools shall continuously measure and report on delay, packet loss, retransmissions, bandwidth use, and service interruptions. In the case of an outage or degraded services defined by specific thresholds, automated alerts and page-outs shall be sent to Contractor's local, dedicated team members who respond to resolve incidents within Service Level Agreement (SLA)-specified parameters. During normal business hours (6 a.m. – 6 p.m.), the engineering and Service Desk teams shall monitor operational status using CA Spectrum and actively respond to alerts. After hours, the Contractor team shall use the automated notification features within the tool to provide the necessary alerts that trigger incident response activities within stipulated SLA parameters (24x7x365).

As part of Contractor's prompt restoration services, Contractor shall report incident response activities to the County using the centralized Contractor Ticketing System. Additionally, on P1 and P2 outages, as well as upon County request, Contractor shall develop root cause analysis documentation and submit it for review. Incident reporting also includes a proactive response to performance or capacity issues, and Contractor's reporting shall clearly identify the nature of the incident or degraded performance and the steps taken to resolve the issue.

Contractor's network performance management shall also use CA Spectrum to provide monitoring. One component of CA Spectrum is CA eHealth, which Contractor shall use to perform trend analysis based on historical measurements as well as current indicators to model, optimize, plan, and report on network services. This tool allows Contractor to meet the County's requirements for speed, reliability, capacity, and quality. CA eHealth also provides real-time and predictive performance analysis capabilities, enabling identification and provisioning of increased bandwidth capacity prior to reaching End-User performance issues on the intranet or Internet.

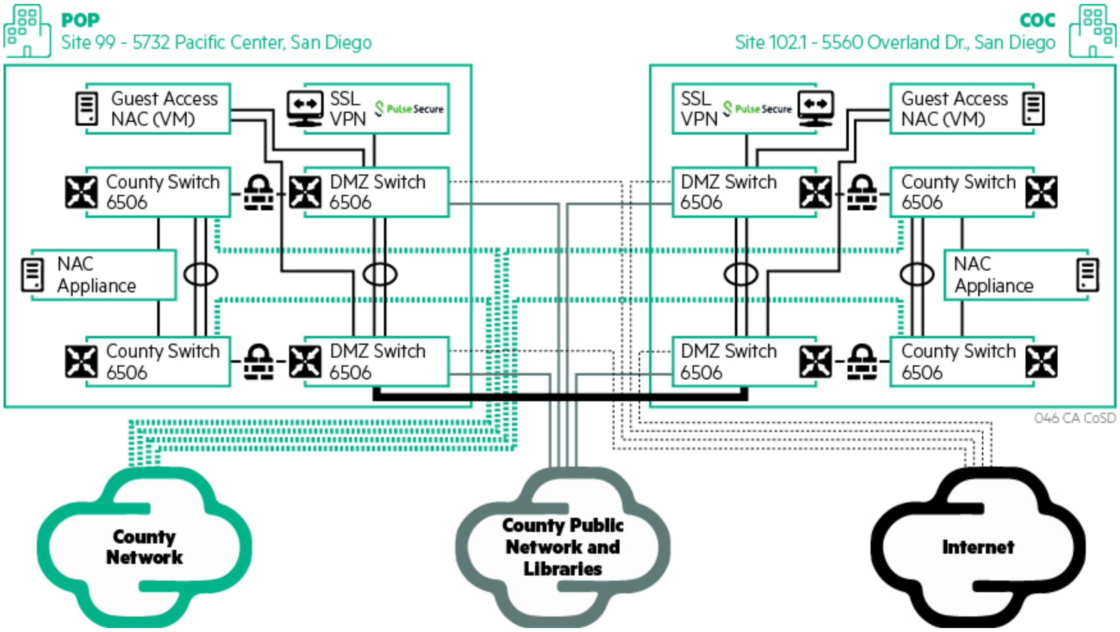
Although CA Spectrum provides passive network monitoring and measurement techniques, Cascade Pilot and Cascade Shark allow active capture, measurement, and analysis of network and application traffic in support of anomaly detection and forensics. The Contractor team shall use these deep packet analysis tools to trend application network performance—establishing thresholds that can be alarmed, correlated, and compared to baselines, enabling a proactive approach to identifying application or desktop issues. Additional network-based tools shall be used to enable a layered approach to trend analysis and event correlation, including Security-based tools such as Palo Alto's Panorama (packet capture and analysis, application identification, traffic volume identification, malware detection, and threat identification); Wireless tools such as Aruba's Airwave (Wireless capacity/ performance); and Voice tools such as Nectar (quality of service [QoS], mean opinion score [MOS], jitter/latency measurement, and round-trip time [RTT] analysis). As Contractor continues to evolve its approach to real-time anomaly detection, new tools and processes shall be evaluated and proposed—improving Contractor's capability to support adjacent frameworks in identifying enterprise anomalies.

Continuous Improvement

Contractor's network shall provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," Contractor's network shall allow any device—managed or unmanaged—to be evaluated, authenticated, and allowed policy-based access. This next generation network shall transform the enterprise by reducing cost and increasing flexibility while improving security and service levels. This new technology shall be expanded in the new term, replacing Opt-E-MAN circuits as well as T1 circuits where possible.

The following figure shows the future state of the centralized, geo-redundant, high-availability network core.

County Network – Future State



County network transformation (future state topology) takes advantage of AT&T's latest software defined network and cloud-based solutions, simplifying the network topology while improving performance, availability, and security.

- Deployment plan for resources and use of facilities

The Contractor network framework team shall maintain infrastructure in County facilities and work closely with the County Technology Office and the Department of General Services to support accessibility and security.

The local life cycle management (LCM) team shall consist of dedicated, full-time resources—many of whom have worked on the County's network for a decade or more. The Contractor network team's primary location shall continue to be in San Diego. All LCM technical, operations, and project management personnel work out of this location. All network services framework components shall rely on the use of the AT&T point of presence (POP) and the County Operations Center (COC). These two geo-redundant sites shall be the core locations holding the centralized communications equipment, appliances, and transport capabilities that securely enable feature-rich capabilities to every business area within the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor team shall apply the following key methodologies in its solution:

- Iterative and bi-modal approaches to solution evaluation: "Start fast," evaluate options, and align solutions to County business needs and long-term strategies; establish proofs of concept, all prior to discussion on cost/price.
- Weekly architecture team collaboration sessions allow a continual transformative approach to be maintained across the entire network framework.
- Weekly Enterprise Architecture Reviews enable cross-framework dialog so that adjacent requirements are understood and delivered.
- Contractor employs ongoing, discipline-specific technical roadmap development.
- Contractor uses a structured refresh process, at 4 years, for core routing infrastructure; and 5 years for LAN switching infrastructure. This approach shall be continually reviewed with the County, making certain that the

refresh activities bring the greatest value to the County, with options for deferral provided while taking service level performance into account.

5.6. Remote Access Services

5.6.1. Process and Procedures

Contractor shall maintain its scalable and secure remote access solution to provide the necessary breadth and depth of functionality. In close coordination with the County, Contractor shall maintain a suite of remote access services via Secure Socket Layer (SSL) connections to satisfy the County’s evolving requirements through numerous transformation initiatives.

Contractor’s experienced, on-site dedicated staff members shall maintain safe, reliable, and secure sessions allowing End-User-role appropriate access to County resources as dictated by County policies and enforced through the use of groups established within Active Directory (AD). This solution set offers an inherent advantage by leveraging the existing AD capabilities. This solution precludes the need to logically connect a disparate system to AD.

To maintain the security and privacy of County resources, Contractor shall establish specific Active Directory group profiles that allow users and capabilities to be directly tied together through specific rule sets for each End-User within the group. Thereafter, Computer Services Registration Form (CSRF) tickets shall provide the direction and authorization needed to assign specific users into their designated profiles. As a result of their specific group membership, users shall be allowed access to a predefined set of resources and precluded from accessing other resources. In this manner, Contractor staff shall enforce County-directed policies.

The Contractor remote access services shall be provided via two independent resource units, Network Persistent VPN, (Virtual Private Network Level 1) and Application Persistent VPN (Virtual Private Network Level 2). These two resource units may be subscribed to stand-alone or in combination and shall apply to the infrastructure, maintenance and support of the hardware and software behind the remote access technology. Base access costs shall be recovered through the Network Access Wired/Wireless RU and shall apply to all County domain registered users.

PulseSecure SSL VPN – Network Persistent VPN (Virtual Private Network Level 1)

Contractor shall maintain geo-redundant remote access gateways from the County Operations Center and the AT&T POP. This solution shall use PulseSecure PSA7000 appliances in the two POPs in conjunction with PulseSecure software loaded on the laptops to facilitate SSL virtual private network (VPN) access into the County domain. This solution shall work with wired and wireless configurations.

Contractor shall continue to evaluate any changes to the environment to identify potential single point of failures and shall work with the County to eliminate them.

This solution shall have the capacity and flexibility to expand, as needed, to support additional users and profiles beyond the existing 2,600 remote users. This scalable solution shall support three profiles—SSLVPN1_D, SSLVPN1_DRW, and SSLVPN1_DRWF. Network access control shall be achieved through a feature known as host checking; the remote host shall be verified as being either a County-owned device or a non-County device and granted domain access as appropriate. For those with full domain access this solution shall provide further granular control by restricting or allowing the use of additional features.

The PulseSecure client loaded on the County-managed laptops (as well as managed mobile devices once that project, which is currently in flight, is completed) shall allow full network access to any and all resources available to the End-User when connected on the County LAN. This client-based connection shall associate each session with a unique IP associated only with the specific End-User's SSLVPN connection for the duration of his or her connection. This connection shall be logged as well as tracked and reported as necessary, and it shall be used during troubleshooting activities that can be isolated to each End-User session.

At the End-User's discretion, a web portal connection shall be initiated by browsing to a URL and authenticating via the End-User's AD username and password. From within the browser session, users shall have the option to perform up to three activities based on their membership privileges:

- **Initiate a terminal services session (remote desktop)** back to their own County desktop (if configured) or another County network device configured to accept terminal service connections. From there, users can perform normal LAN activity within that remote desktop session as well as create bookmarks for quicker access in future sessions.
- **Browse to County intranet sites** (such as Insite) using the browse function within the web portal window. Users can create bookmarks for these sites on their main web portal page.
- **Access file shares** that users have been granted permission to access, and create bookmarks to these shares.

All of these actions take place within the web portal window. Anything done outside of that window, including web browsing using a separate window or tab, does not flow to the County network.

There are two remote access security features available for transformational use:

- **Security posture evaluation** assesses a device's security posture by determining the presence, versions, and levels of antivirus, spyware, and malware protection as well as operating system (OS) version and patch level, software patches, and disk encryption.
- **Role-assigned remediation** allows the restricted network access of devices for the sole purpose of performing remediation of any failed checks found during the security posture evaluation.

.

Another feature of the PulseSecure solution is direct support for smartphones and tablets provided by installing the PulseSecure mobile application onto these types of devices. However, due to inherent limitations with these mobile devices at present they cannot be configured to automatically sense the unavailability of one gateway and connect using the alternate.

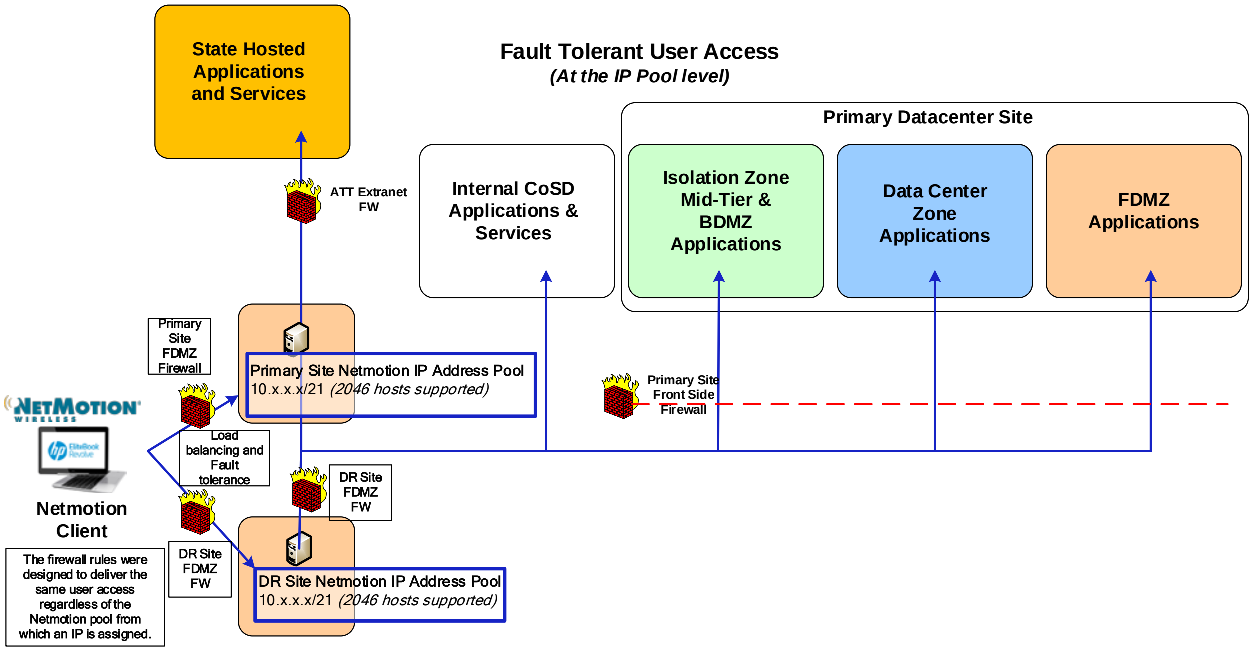
Currently the PulseSecure mobile client is not "connection aware" and is unable to dynamically reconnect to a secondary gateway in the event the connection to the primary gateway fails. Contractor has initiated feature requests and roadmap discussions with PulseSecure to address the manual failover inherent to the mobile VPN solution for the County, which shall be implemented at no additional cost to the County. If this feature does not become available in the first 9 months of the Agreement term, the Contractor shall evaluate and implement a global load balancing solution such as F5's GTM (Global Traffic Manager) by the end of CY 2 of the Agreement at no additional cost to the County. This solution shall involve the installation of two virtual appliances leveraging Contractor's existing virtual infrastructure at both the POP and COC. This solution also possesses the potential to be leveraged for other services such as Mutare Voicemail to Email Service and could extend the capability of global load balancing to all solutions offered externally from the COC and POP.

NetMotion – Application Persistence (Virtual Private Network Level 2)

Contractor's remote access solution shall include application-persistent capabilities through its deployment of NetMotion Mobility VPN. Similar to the SSL VPN System, the application-persistent capabilities of NetMotion are enabled by assignment to the correct group profile, which also determines which specific application an End-User may access. Currently, there are approximately 1,200 mobile workers who require VPN connectivity and application persistence to support their business objectives and who require connectivity to the County as they roam between networks. In the new single data center model, NetMotion shall be configured for high availability with redundant servers load balanced and takes advantage of the built-in redundancy within the data center for storage, network, electrical, etc., as well as the redundant connections to the data center.

Contractor shall deliver an environment that supports mobility session persistence for County mobile workers as they roam wireless carrier networks throughout their business day. Also, it considers the internal County and external County network destinations to which mobility users must connect for successful business productivity. Contractor key objective is to manage the mobile End-User traffic efficiently so that business traffic traverses the links to the applications within the data center and internal County networks, but non-business traffic is redirected through the wireless carrier network or broadband connection. This capability is known as split-tunneling, and it maintains the performance and security of the County's network. A depiction of the logical solution architecture is presented in the following diagram

Figure 2. Fault Tolerant User Access


State Hosted Applications and Services
Fault Tolerant User Access
(At the IP Pool level)
Primary Datacenter Site
ATT Extranet FW
Internal CoSD Applications & Services
Isolation Zone Mid-Tier & BDMZ Applications
Data Center Zone Applications
FDMZ Applications
Primary Site FDMZ Firewall
Primary Site Netmotion IP Address Pool
10.x.x.x/21 *(2046 hosts supported)*
Primary Site Front Side Firewall
NETMOTION WIRELESS
Load balancing and Fault tolerance
DR Site FDMZ FW
Netmotion Client
DR Site FDMZ FW
DR Site Netmotion IP Address Pool
10.x.x.x/21 *(2046 hosts supported)*
The firewall rules were designed to deliver the same user access regardless of the Netmotion pool from which an IP is assigned.

Remote Access Services

- Deployment plan for resources and use of facilities

For continuity of Contractor's existing geo-redundant network and remote access capabilities, Contractor shall use the AT&T POP in the County as well as the County's Operations Center to hold the Mobile Access Gateways, VPN appliances, and to facilitate circuit terminations. The NetMotion application-persistence solution shall be hosted on highly available and load-balanced virtual machines within the primary Contractor data centers. Contractor shall maintain the NetMotion solution infrastructure in accordance with the standard procedures and policies, while supporting the application with guidance from NetMotion.

Working from its local facility, Contractor's SMEs shall monitor, support, and maintain the remote access services. Any client side issue support shall be initiated through Contractor's Service Desk process.

- Key methodologies and processes in solution including year-to-year continuous improvement

Through the Contractor team's routine involvement within the Enterprise Architecture Forum meetings, the Contractor team's SMEs shall maintain an in-depth understanding of the County's remote access needs and proactively prepare Solution Design Documents for County approval. Thereafter, Contractor's planning and testing of the solution shall allow activations to go smoothly, with back-out plans executed if required.

When a new End-User or group of users requires remote access, Contractor shall gather requirements and determine the type of access needed. For SSL VPN and Application Persistence users, new users shall be placed into an Active Directory group with the appropriate level of access and security. For Mobile Access Gateway users, a Mobile Device Management (MDM) solution shall provide the appropriate level of access and security. Contractor shall continually evaluate new technologies and vendor roadmaps so that the most secure and reliable system with the highest performance is available to the County. The Contractor Service Desk shall post text-based information into Tier 0 repositories, and the Contractor network team looks forward to working with the County to advance into video-based Service Desk files in order to better reach Contractor’s customer support community.

Hardware associated with remote access shall be refreshed on an ongoing 4-year cycle. This approach shall be continually reviewed with the County, making certain that the refresh activities bring the greatest value to the County while offering continuous improvement to the service.

On a continual basis Contractor shall create, maintain, and update End-User training documentation and tips as well as associated Service Desk scripts pertaining to the remote access to match the version and features of the product.

To allow the maximum return on the County’s investment, Contractor shall make full use of the existing solution set, which can adapt to the County’s future requirements. However, as the technology and requirements landscapes evolve, Contractor’s SMEs shall evaluate and propose new solution sets as needed to meet the County’s needs and joint objectives

Network persistence and application persistence in Remote Access Services.

In support of the County’s vision of a “Government without walls,” Contractor shall maintain a remote access solution that leverages redundant infrastructure with software enabled network and application persistence. This multiplatform solution was designed and delivered to meet specific business purposes, starting with the functionality of SSL VPN and then expanded to provide application persistence for mobile users that actively interact with enterprise data while physically in motion and in turn are exposed to the connectivity interruptions that can occur across carrier mobility networks.

Contractor shall maintain the Pulse Secure SSL VPN service.

As remote access technologies continue to evolve, Contractor shall consolidate the network and application persistence.

User experience, impact to business associated with a change in solutions, as well as providing the proper levels of support shall be carefully weighed for any and all solutions under consideration.

Contractor’s approach is to take a transformative approach to this goal, evaluating the best options for the County in the term of the agreement. Contractor shall continue to closely monitor industry trends, vendor roadmaps, and innovation in the remote access space to properly evaluate and select the best solution for the County. Contractor shall work closely with vendors to determine the optimal solution in terms of reliability, usability, functionality, features, and the ability to make full use of the redundant network architecture to preclude any single points of failure as part of the solution.

5.7. Voice Services

5.7.1. Process and Procedures

Voice Services

Each transformational activity shall be initiated through the Enterprise Architecture Forum, where Contractor shall provide ongoing architecture and management resources to facilitate the planning of upgrades, refresh, and strategic plans related to Contractor's voice services. In this forum, Contractor shall perform the following:

- Maintain ongoing collaborative voice and unified communications roadmaps and architectural standards, with yearly reviews/revisions, enabling the continued advancement and adoption of emerging technologies.
- Identify single-point failures within the voice architecture and propose solutions for County consideration.
- Make recommendations to reduce County usage costs.

VoIP Services

Contractor shall leverage the existing network infrastructure and build upon it by replacing older TDM and PBX technologies with Voice over Internet Protocol (VoIP) solutions that tie seamlessly into capabilities already implemented on the County network. As with other transformations, service changes must be completed within realistic cost constraints that provide demonstrable return on investment. Due to these real-world restrictions, Contractor's solution includes significant reuse of existing assets that are current technology and well inside of the technology refresh cycle. Contractor shall reuse the major core voice-related appliances and associated licenses shown in the following table.

Major Core Voice-Related Appliances and Associated Licenses

AVAIL	IN USE	TYPE	DESCRIPTION
26,305	23,901	Aura Communication Manager-Core	Core license for CM stations
26,305	166	EC500	Extension to cellular
26,305*	277	One X Communicator	Softphone on desktop
26,305	0	One X Mobile	Softphone on mobile device
26,305	1	One X Communicator for Lync	Softphone on desktop for Lync integration
2,647*	2,647	Call Center Elite	Core call center software license
321	284	Elite Multichannel	Software for screen pops at ACCESS
484	452	Avaya Call Recording	Software for recording/ storage of agent/ customer voice calls
1,051	2,883	Call Management Agent	Per agent license for CMS
125*	309	Call Management Supervisor	Per supervisor license for CMS
12*	9	One X Agent	Desktop client phone for agents
175*	175	AAEP port	Experience Portal port license
181*	181	AAEP CM Connection	Experience Portal to CM connection license
82*	82	Enhanced Call Classifier	Experience Portal call classifier license
117*	117	Nuance ASR	Experience Portal speech recognition license
117*	117	Nuance TTS	Experience Portal text to speech license
1,000	481	Mutare EVM	Mutare voice mail to email
1,000	481	Mutare giSTT	Mutare voice mail to text transcription
17,000	16,941	Modular Messaging	Voice mail licenses

AVAIL	IN USE	TYPE	DESCRIPTION
26,305	200	Session Manager SIP connections	SIP licenses
3,758	200	Session Border Controller Trunk	SBC licenses for SIP connections
3,758	2	Session Border Controller Stations	SBC licenses for SIP connections

To support Contractor’s transformational objective for VoIP services, Contractor’s SMEs shall work within the architecture forums and draft Solution Design Documents for the site Transformations. Contractor’s formal solution design approval shall then be used by its project management team to develop implementation strategies and communicate with site-based County resources to upgrade each specified facility to VoIP services. These changes reduce equipment footprint at each of the sites, while dramatically reducing the overall power consumption and increasing availability and reliability. Equally important, the upgrade improves the End-User experience by reducing trouble tickets regarding set-based issues—such as speaker and cord problems—and also provides new feature sets.

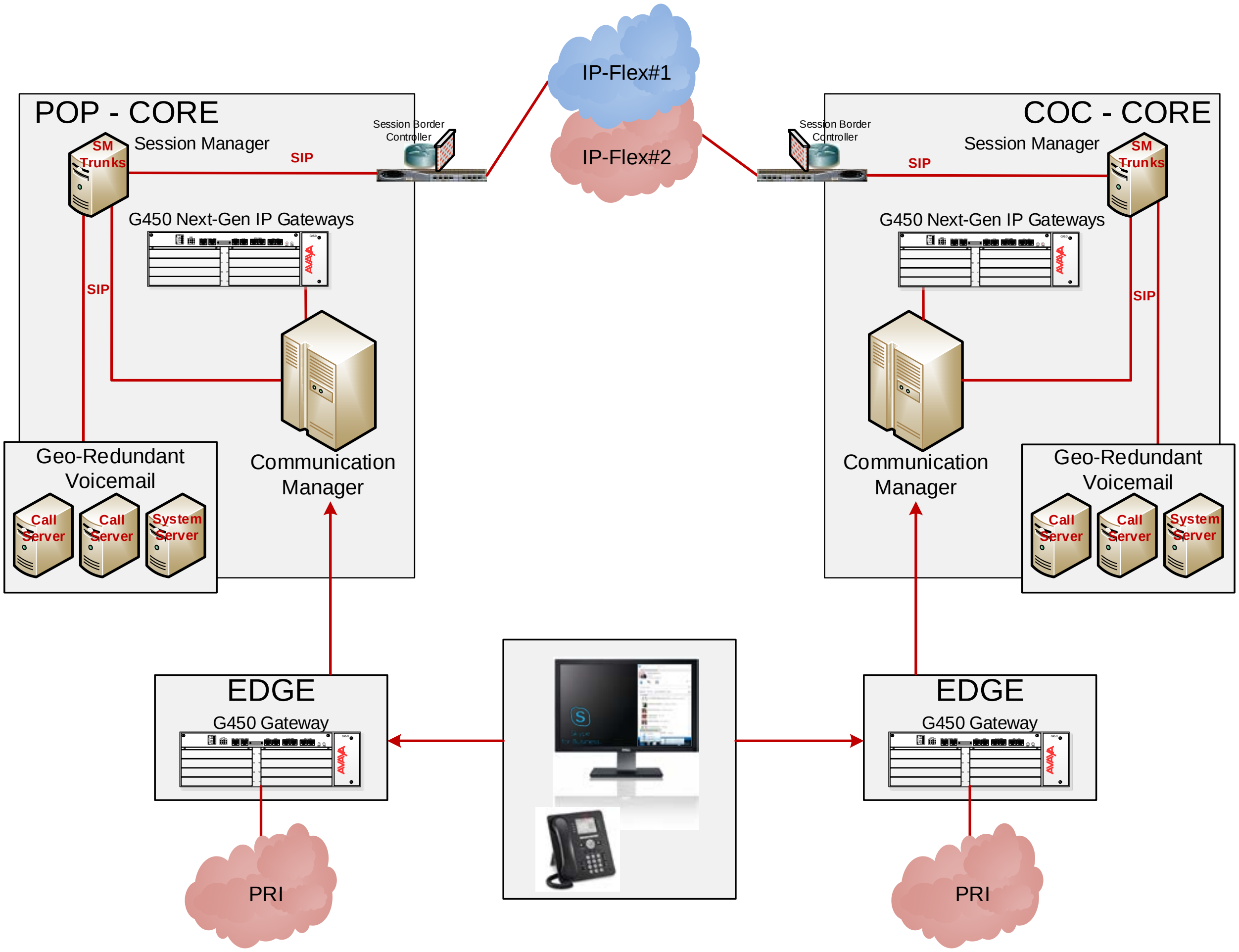
As a part of this Transformation project, each site shall also be migrated to a new E911 service, so that first responders have the necessary site and call location detail in the event of an emergency.

All new County sites shall continue to be implemented with VoIP services as part of Contractor’s ongoing efforts to continuously maintain technical currency and modernization of these services.

Geo-redundant Voice Mail

Contractor shall leverage a geo-redundant voice mail platform to provide a standardized voice mail experience across all County locations where enterprise voice services are offered. This solution shall include a phased migration of Centrex users to the new platform as these services are brought into new voice services standards. The following figure is a representation of the high-level topology of the voice mail solution that shall be in place at the time of the Agreement if approved.

High-Level Topology



AVST with Neverfail provides geo-redundant, high-availability voice mail services.

Voicemail to Email Services

Contractor shall continue to support Mutare speech-to-text service for transcribing voice mail messages into text with delivery to the End-User via email along with a .wav file to the County End-User email on a per-request basis by the County. This service is provided via a cloud-based platform.

Unified Communications

Contractor's team shall expand the integrated desktop and handset functionality as part of Contractor's efforts to integrate voice services into unified communication services. These enhancements shall include complete call control from the Lync or Skype for Business client with the following key features:

- Click to call and click to answer from Lync or SfB
- Search and click to call from Outlook contacts
- Outlook contacts match and screen "pop" click-to-conference.

Avaya Communicator Softphone

Contractor shall offer Avaya Communicator softphone functionality. This service allows remote and teleworkers a full featured software client, deployed upon request to their County provided device. Leveraging the connectivity provided by a direct LAN connection or PulseSecure VPN/Netmotion, Avaya Communicator allows End-Users to make and receive calls from their designated County telephone number at their desk and remotely via a headset.

On-net Dialing and SIP Trunking

Contractor's solution to voice interconnectivity shall use the robust, fault-tolerant solution deployed within the data network to provide resilient connectivity not only within the County domain, but as needed to support cloud-based solutions. This connectivity facilitates improved end-to-end collaboration and also reduces operational costs by implementing efficient local and long-distance dial plans. Contractor shall include capacity expansion of the existing SIP-trunking internally and externally for increased efficiencies. As an immediate objective, Contractor's team shall expand the capacity of SIP services, configuring them to support not just local calls but also long-distance and toll-free (800) calls. Contractor shall eliminate usage charges for all outbound domestic calls from the enterprise and reduce the usage charges for toll-free 800 inbound calls.

Centrex Migration

AT&T has developed a Transformation approach to migrate a majority of these users/stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed over the term of the Agreement. This effort is planned for implementation early in the term as a Transformation initiative and is included in the Voice Services.

The first transformational step to migrate Centrex users shall include the deployment of stand-alone IP-based telephones at sites with existing data network functionality. This solution provides VoIP telephone sets at the remote site, centrally managed by the Avaya geo-redundant voice cores at the AT&T POP and County Operations Center. While these sites do not have local survivable gateways, they take advantage of the data network for their connectivity to the enterprise voice infrastructure. Through this migration, individual stations shall be converted to the Avaya enterprise standard, where they are provided new centralized voicemail and Unified Communications functionality options as well as a new telephone set.

Basic/Simple IVS Solutions

Contractor shall provide the support of Auto Attendant and Automated Call Distributor services as a right to use feature for subscribers of Voice Services. This basic functionality is inherent to the Avaya enterprise telephony network. Contractor shall enable 39 previously billed "Simple" IVS resource units to consume the service no additional charge.

411 Operator Services

In 2015, AT&T upgraded the IVR that supports the County 411 information line, providing additional self-help capabilities and bilingual voice recognition. This new service has provided improved efficiency in delivering County and public users with County information. Contractor shall continue to provide these services, including a live operator option for users and constituents who "zero" out of the IVR. Over the life of the Agreement, additional recommendations shall be developed and proposed to enhance and improve this important service.

800 Toll-Free Services

Contractor shall ensure that toll-free services for publicly dialed County telephone numbers are supported by AT&T and provided at a significant price reduction relative to current rates.

- Key methodologies and processes in solution including year-to-year continuous improvement

For End-User support within the new contractual service level requirements, the Contractor team shall continue its multi-tiered service and support structure. This structure provides the appropriate skills at each level to handle incidents, coupled with a clearly defined escalation management process to facilitate proper incident response and resolution. In addition, Contractor shall use a complete set of automated tools, which drives quicker response and resolution and minimizes impact.

Each platform/service type shall use a predefined set of operational processes to achieve customer satisfaction and service levels. The Contractor team shall leverage the Nectar Unified Communication Management Platform to access knowledge modules to assist with identifying and resolving issues. Also, Contractor shall leverage an internal SharePoint Services Knowledge Base that provides a customized set of knowledge and process tools specifically reshaped over time for Contractor's internal use only to support voice service response team. The Contractor team shall maintain its voice-specific internal SharePoint Wiki that has complete infrastructure documentation organized by site.

5.8. Network Security Services

5.8.1. Process and Procedures

Network Security Services

- Description of solution to meet the requirements

Contractor shall leverage the existing security infrastructure solution to further improve the security posture of the County network. The following components shall be included in Contractor's solution:

- **Palo Alto next-generation firewalls with unified threat management capabilities.** These appliances provide not only firewall services, but they also provide intrusion detection/prevention (IDP), spyware and AV filtering, and web content filtering. Automated, daily threat updates allow the County network to be protected against the very latest in malicious content and activities. Extensive reporting in this solution enables deep dive views of network communications to highlight the possible effects on network performance. This solution also provides automated alerting of possible malicious activity for immediate investigation and remediation.
- **Websense cloud-based content filtering.** This technology further protects County assets, even when outside the County domain. By replicating content-filtering policies in use on the local County network to the cloud-based service, Contractor is able to support continuity of protection across all avenues of connectivity in use by County personnel, regardless of their physical locale.
- **Websense Data Loss Prevention (DLP) for web channel and data in motion.** This service prevents sensitive data (personally identifiable information [PII] for instance) from being transmitted outside of the County network in unencrypted communications or copied to a removable device (i.e., thumb drive).
- **Advanced Distributed Denial of Service (DDoS) detection and protection.** This service protects County Internet circuits and provides security event analysis and correlation via live 24x7x365 monitoring.
- **Tenable Security Center.** Continuous perimeter scanning provides a close to real-time view of supported and non-supported inventory, including real-time threat updates and monitoring of vulnerabilities and risk, as well as close to real-time asset status updates. This provides an improvement to the snapshot in time information that is currently available.

Transformation Opportunities

As part of Contractor's dedication to continuous improvement for the County, Contractor shall support and maintain the following efforts:

- **Application-level security policies.** By moving from port/protocol-based firewall policies to application-based policies the tools can fully inspect traffic flows. This type of technology safeguards against programs attempting to use non-standard ports to circumvent port/protocol-based security. The Contractor team may refine security policy to data flows, as well as determine the types of applications in use on the County network. This enables Contractor to provide more in-depth assessments and recommendations for network enhancements.
- **User identification.** By providing positive identification for each End-User tied to a data transmission, firewall policies can be written to allow authorized network communications based on End-User ID rather than an IP address. Consequently, the policy is in effect for the End-User, regardless of his or her location on, or entry point into, the County network. This solution eliminates the need for static IP addresses for firewall policy mapping—thereby providing better policy management without the need to map policies to entire subnets to accommodate the mobile nature of today's workforce.
- **Active Directory group-based policies.** Much like End-User identification, AD-based policies allow for the mapping of security policies to specific groups created within AD. This allows for a security policy to be applied to all users who are members of an AD group, regardless of where they reside on the County network. For example, if a member is added to the HR group then he or she automatically inherits the security policies applied to that group without having to have a firewall change made to accommodate him or her specifically. As a result, Contractor's SMEs have greater flexibility in mapping security to End-User roles without increasing complexity in either process or implementation.
- **Network Access Control (NAC).** This capability provides appropriate levels of network access based on the device being connected. County-managed devices are given full access to the County network just as they are today. Non-County devices are segregated on the County network and allowed only access to the Internet unless otherwise authorized through a formal review process.
- **Integration with the County's PKI solution.** These integrated solutions guarantee that only County-authorized devices are able to connect using County wireless networks or via the County's SSL VPN solution. This approach effectively isolates the network from exposure to non-County managed devices that pose a security risk.
- **Websense Data Loss Prevention (DLP).** The DLP solution is already in place for data in motion and web channel, protecting against the release of sensitive data onto the public network or transfer of data to removable devices. The next phase of that enables the scanning of repositories to identify sensitive data being stored in non-secure locations.

- Deployment plan for resources and use of facilities

All hardware and software used to provide network services from the AT&T POP location shall be contained in a secure location, accessible only by AT&T personnel or those they escort. All personnel having access to County associated devices at the AT&T POP shall have undergone background checks and verification. Security measures shall include guarded access, with signature and ID required for admittance along with biometric security.

Access to network services hardware and software located at County facilities is to be managed by the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall evaluate patches and updates as they are made available to determine their applicability to the County environment and shall deploy them immediately as needed.

The continuous 4-year refresh cycle shall apply to security hardware as it does to all network refresh activities. The hardware and systems shall be continuously evaluated so that they can meet the requirements of the County's high-speed network and are upgraded as needed.

Contractor shall perform the configuration of the hardware and software using industry best practices—resulting in hardened, or locked down, systems. Contractor shall remove default usernames and passwords and disable unnecessary services, and all management communications to and from the devices shall be via encrypted connections.

- Use of Tools

Contractor shall provide and maintain a centralized management platform to deliver strict change control along with powerful reporting and alerting capabilities and automated notification of security events.

Through AT&T's vendor, Security on Demand, Contractor shall capture these threats by performing analysis against the data, including behavioral analytics, to determine whether there is a potential threat. If such a threat exists, or further analysis with the LCM team is required, then a ticket shall be generated or a call placed directly to Contractor's dedicated security staff for high severity issues.

The logging mentioned above, as well as all of the logging from the Contractor security devices, shall be fed into the security information and event management (SIEM) solution for analysis and triangulation against other security data sources such as data center firewalls and intrusion prevention systems/intrusion detection systems (IPS/IDS).

Automated email alerts shall also be delivered daily to the dedicated Contractor security staff by Contractor's Palo Alto environment, where additional analysis shall be conducted and fed to the Cross Framework security team and Cross Framework capacity and performance team. Finally, Contractor's Security team shall use these tools to develop recommendations for evaluation by the Contractor CISO and County CISO.

From this analysis, Contractor shall take actions to include, but not be limited to, scanning of devices, removal from the network and reimaging of desktop devices if necessary (for County assets), and configuration of network or URL blocking and tuning of threat signatures. Contractor shall conduct investigations to determine whether hosts have fallen victim to malicious activities and what the impact or spread of those may be. All investigative reports shall be provided to the County for its review.

In addition, monthly reporting shall be provided to the County CISO for review with PMO Security on both threat alerts and URL blocking taking place in the County environment. This allows both trending analysis and the development of future security strategy roadmaps.

5.9. Video Conferencing Services

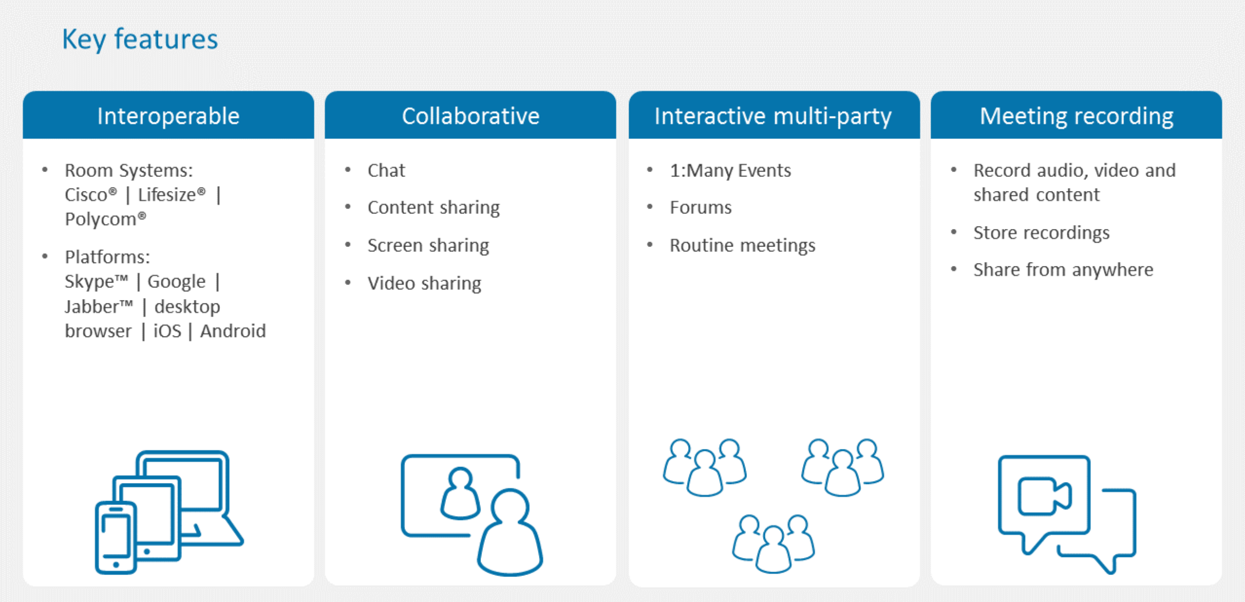
5.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall continue the use of existing video conferencing capability in conjunction with a cloud-based solution to fulfill all of the County video conferencing requirements. To remain compliant with required equipment refresh cycles, part of Contractor's solution replaces the Tandberg Management System (TMS) and Video Conferencing System (VCS) with the Cisco Unified Communications Manager (CUCM) virtualized appliances, which shall be implemented in a geo-redundant configuration between the AT&T POP and the County Operations Center.

To fulfill the need for a fully integrated video teleconferencing solution, Contractor shall provide AT&T Meetings with BlueJeans. This solution offers a cloud-based video bridging capability that can integrate services like Skype for Business and Google Chat with traditional standards-based room video systems. The system is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing. Features of this integrated solution is depicted in the figures below.

BlueJeans via AT&T



Key features

Interoperable

- Room Systems: Cisco® | Lifesize® | Polycom®
- Platforms: Skype™ | Google | Jabber™ | desktop browser | iOS | Android

Collaborative

- Chat
- Content sharing
- Screen sharing
- Video sharing

Interactive multi-party

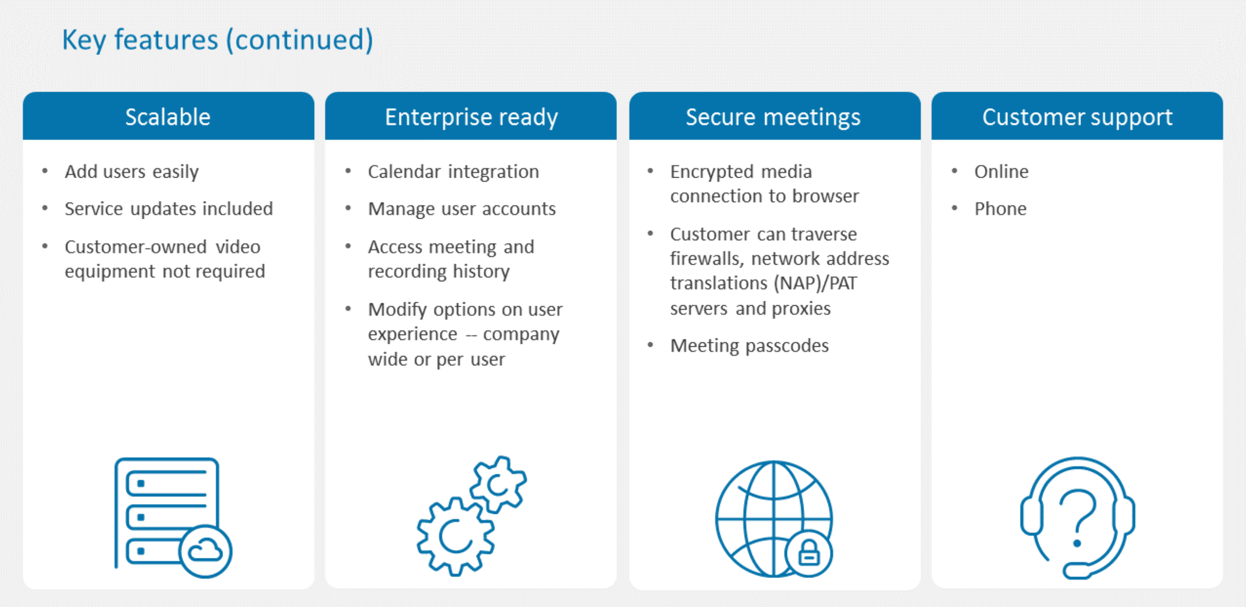
- 1:Many Events
- Forums
- Routine meetings

Meeting recording

- Record audio, video and shared content
- Store recordings
- Share from anywhere

The hosted Meetings with BlueJeans via AT&T provides full interoperability across many platforms and allows for many types of collaborative, real-time interaction.

Hosted Meetings with BlueJeans via AT&T



Key features (continued)

Scalable

- Add users easily
- Service updates included
- Customer-owned video equipment not required

Enterprise ready

- Calendar integration
- Manage user accounts
- Access meeting and recording history
- Modify options on user experience -- company wide or per user

Secure meetings

- Encrypted media connection to browser
- Customer can traverse firewalls, network address translations (NAP)/PAT servers and proxies
- Meeting passcodes

Customer support

- Online
- Phone

The hosted Meetings with BlueJeans via AT&T scales easily both internally and externally, while providing additional enterprise and security capabilities.

This Meetings with BlueJeans solution leverages the availability of existing videoconferencing units around the County and facilitates interoperability with the existing Skype for Business clients for extended telepresence. Users can participate from anywhere using any device—with a dedicated app, a web browser, or the Skype for Business mobile application.

From a desktop/laptop/tablet/smart phone End-User's perspective, the Meetings with BlueJeans experience is as easy as clicking on a link in an email or a meeting request. The Outlook plugin adds the capability to schedule meetings using a personal meeting ID or a dynamic meeting ID. Users can also edit default meeting preferences and add/edit/cancel meetings. The additional support for delegate scheduling allows executive support personnel to schedule meetings on behalf of executive staff. From an existing Cisco videoconferencing unit, an End-User simply dials by inputting the IP address as listed in the invitation.

Additionally, the Meetings with BlueJeans hosted solution allows numerous customizations, including the ability to set language preference, meeting passwords, entry tones, meeting security controls, and more via the web-based End-User interface. Features such as the high-definition content support, video sharing, and the ability to record meetings coupled with the integrated encryption allow the County to conduct video meetings securely as desired today and into the future.

- Deployment plan for resources and use of facilities

Contractor's solution shall use the existing video conferencing solution set and the associated facilities that house the equipment, including core infrastructure in the AT&T POP and the County Operations Center. Furthermore, Contractor's existing local staff shall continue to support the video conferencing services as well as all of the other framework components from its County location. This local staff shall also be responsible for continuous development, maintenance, and updates of all items associated with video conferencing, including Service Desk scripts, training documentation, and processes for End-User support—and this staff shall continually provide new and updated material to support operational needs.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's SMEs shall continue to evaluate solutions and introduce them through the weekly network architecture meetings and thereafter through the Enterprise Architecture Forum. These iterative processes allow Contractor's solutions to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals as well as maintain consensus.

The Contractor team shall use insight gained from the ongoing operation and maintenance of the infrastructure to assess potential transformational, refresh, and upgrade activities. If other SPOFs are identified and remediated, then Contractor's SMEs understand the processes and documentation to effect the change with minimal effort by all parties involved. Contractor's local, dedicated team provides the coordination of resources necessary to plan, design, and implement the video and archiving solution.

When Contractor receives an Install/Move/Add/Remove (IMAR) request, it shall gather information and design a solution to present for the County's approval. Once approved, Contractor shall order, receive, and stage the equipment and other necessary components for installation. Contractor shall coordinate the installation date with the End-User or business unit and dispatch a technician to complete the installation.

The BlueJeans integrated video teleconferencing solution shall include a 100-host license, where designated video conferencing hosts are to be identified by the County. These 100 licenses represent simultaneous conferences, as only one licensee is required per conference. These licenses are dynamic and can be changed in real time to different users via the scheduling portal.

Over the life of the term, the wider adoption of standards-based systems like Skype for Business/O365 along with anticipated industry enhancements may shift the solution for multi-platform video teleconferencing. The Contractor believes that the Microsoft's planned development of multi-platform transcoding via a Skype for Business mediation server positions the County to move towards a Skype based standard for all video teleconferencing services. The Contractor shall work with the County to evaluate such options and make recommendations accordingly.

Integration of desktops into Video Conferencing Services.

Contractor shall provide AT&T Meetings with BlueJeans, a hosted video bridging capability that can integrate services such as Skype for Business and Google chat with traditional standards-based room video systems. This enables fully integrated business-to-business (B2B) video calling and is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing.

Additionally, as the County increases its use of video teleconferencing, AT&T NetBond enables videoconferencing traffic to be redirected off of the ISP connections to a private multiprotocol label switching MPLS connection to support additional performance, scalability, and security above and beyond the integrated encryption. The NetBond to BlueJeans cost is not included in the Baseline Resources Units.

BlueJeans users can also benefit using Outlook plug-ins. An End-User can schedule meetings using a personal or dynamic meeting ID, edit default meeting preferences, and add, edit, or cancel meetings. Delegate scheduling provides administrative staff the ability to schedule meetings on behalf any team member. To set up a call, the End-User simply inputs the IP address as listed in the invite.

The BlueJeans platform allows numerous customizations including the ability to set language preferences, meeting passwords, entry tones, and meeting security controls via the web-based End-User interface. Features like high-definition content support, video sharing, and the ability to record meetings, coupled with the integrated encryption, provide secure meetings for County users.

5.10. Video Streaming and Archiving Services

5.10.1. Process and Procedures

Video Streaming and Archiving Services

- Description of solution to meet the requirements

To support the increasing video distribution needs of the County, from both live and on-demand perspectives, Contractor shall use the existing Granicus System as a compliant starting point. This provides continuity and stability as more future-focused technologies are investigated.

- Deployment plan for resources and use of facilities

Contractor shall use the two current core facilities already in use at the AT&T POP as well as the CAC as a primary video content sourcing location. Furthermore, this solution shall use the existing network infrastructure to support an efficient video distribution capability. Contractor's local, dedicated staff shall be active liaisons on behalf of the County, and Contractor shall select external cloud providers so that required service level requirements are continually met.

- Key methodologies and processes in solution including year-to-year continuous improvement

Going forward, Contractor shall achieve consensus on the Video Streaming and Archiving Services Roadmap by vetting or via recommendations in the weekly network architecture meetings—and thereafter via the Enterprise Architecture Forum. Use of these iterative processes allows Contractor's solution to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals while maintaining consensus. As such, Contractor's SMEs shall continue their active participation within these forums as well as their participation in other meetings to stay abreast of customer needs, report on changes in technology, and propose low-risk solutions to meet County business requirements. Furthermore, the Contractor team shall use insight gained from the ongoing operational and maintenance aspects of the infrastructure to assess potential transformational, refresh, and upgrade opportunities. Contractor's local, dedicated team shall provide the coordination of resources necessary to plan, design, and implement the video and archiving solution. All work efforts and problem reports shall flow through the existing processes in place for support of the County's network by the AT&T LCM team.

On a continual basis, Contractor shall create, maintain, and update End-User training documentation and tips, as well as associated Service Desk scripts pertaining to the solution, to match the version and features of the product.

- Use of Tools

As new appliances and capabilities are expanded within the existing data network, the Contractor team shall expand the use of CA Spectrum and eHealth to monitor the operational status of the appliances and the bandwidth usage so that the ongoing operational capabilities are met as compared to the service level requirements. High-grade analytics shall provide viewer statistics along with performance information to provide a clear picture of performance and where possible trouble spots within the infrastructure may be occurring so that Contractor can take near-real-time corrective actions.

5.11. Mobility Infrastructure Services

5.11.1. Process and Procedures

Mobility Infrastructure Services

- Description of solution to meet the requirements

AirWatch MDM Infrastructure

All components of Contractor's industry-leading AirWatch Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for the County shall be maintained and supported in a fully geo-redundant configuration. The AT&T MDM solution shall use a cloud-based AirWatch Software as a Service (SaaS) MDM/EMM solution integrated with on-premise AirWatch Cloud Connectors (ACCs) deployed into the AT&T POP and the County Operation Center. These ACCs in turn shall interoperate with the County's Active Directory infrastructure for End-User authentication.

Contractor shall maintain and support its proxy services between County Enterprise Systems and the SaaS MDM/EMM cloud, as well as application gateways services for developed or acquired applications, to internal County resources from mobile devices using Mobility Infrastructure Services.

Due to the nature of the cloud service and the geo-redundant configuration of the on-premise infrastructure, the AT&T MDM solution has no identified single points of failure.

Mobile User and Device Profiles

Contractor shall maintain and support the three profile groups established within AD: The Corporate Single Device, the Corporate Multi Device, and the Bring Your Own Device (BYOD). These profile groups can be expanded as business needs are defined, where the Contractor team simply adds a group profile within AD recognized by the AirWatch Platform. Users are identified through CSRFs and placed into the respective groups.

Contractor shall support County "corporate owned" devices and BYOD in a reliable and secure manner and shall manage them according to specific County-defined policy.

After being enrolled within the designated group, when a mobile device End-User requests access to the County domain, the End-User is certified against the AD; thereafter three profiles (Passcode, Restrictions, and Exchange) are pushed Over the Air (OTA) to the device.

The AirWatch cloud-based solution provides central management and control of all mobile devices and mobile applications from a single unified console. This console also allows Contractor's solution to enforce County-approved device policies for security and data protection across the End-User population of County and BYOD mobile devices. For instance, Contractor's solution provides the County Mobile Application Store for developed or acquired mobile applications and limits the access to the applications to only County-managed MDM devices.

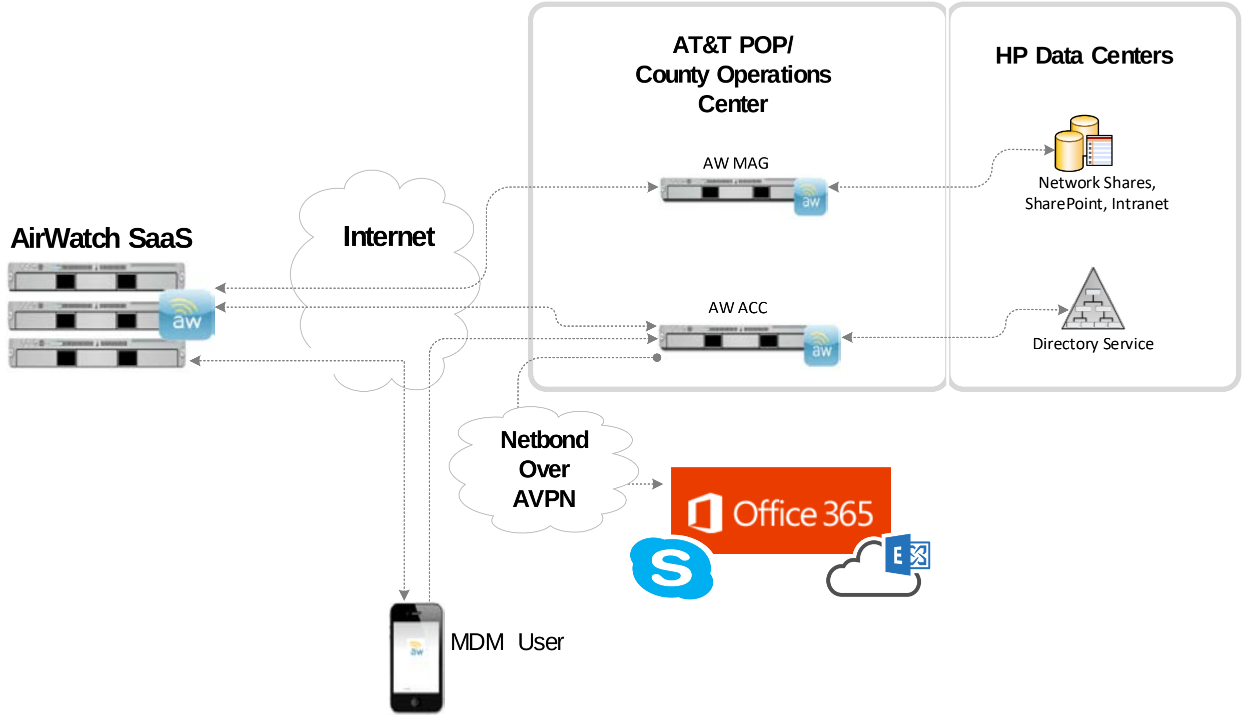
Mobile User and Device Authentication

Contractor's solution shall enable client authentication, encryption, and message signatures to secure corporate resources and connections. AT&T's SaaS MDM/EMM solution shall integrate with third-party Certificate Authorities and Public Key Infrastructure (PKI) providers in cloud and on-premise deployment models. AT&T's SaaS MDM/EMM solution shall distribute Symantec Managed PKI certificates to corporate managed mobile devices for mobile VPN authentication and integration. Future roadmap capabilities shall include the potential for PKI integration delivered via AirWatch MDM for access to County staff Wi-Fi as well as seamless integration with the PulseSecure Mobile VPN application.

AirWatch Integration with O365

As a Transformation initiative, Contractor plans to migrate Exchange to the O365 cloud. Although the current integration from the AirWatch SaaS MDM/EMM solution to the County infrastructure for email services is premises based with integration to services in the data center, the solution can be configured to integrate to Office 365 with Outlook via an AVPN with AT&T NetBond service. Contractor shall ensure that AT&T and its Mobility Solution Services team engages in this migration effort, updating design documentation and making certain that End-User connectivity to email is enabled as the services are migrated to the cloud. The figure below presents the reconfiguration of the AirWatch premise-based infrastructure.

AirWatch



The AirWatch premise-based infrastructure is reconfigured as part of the migration of Exchange to the O365 cloud, enabling email access to MDM-compliant devices.

- Deployment plan for resources and use of facilities

Contractor shall use the existing, knowledgeable AT&T Lifecycle Management team located at 7337 Trade Street in San Diego, California, along with AT&T's leveraged Mobility Support Services (MSS)/Application Service Desk (ASD) organization to continue to support the premise- and cloud-based AirWatch infrastructure.

The ASD is composed of experienced, industry-certified professionals who provide hands-on, comprehensive, and proactive managed services and technical support. In addition to the ASD, the local team also retains a highly skilled mobility consultant, who has intimate knowledge of the County AirWatch tenant and continually provides support and guidance on operational and strategic initiatives.

Facilities involved shall include an AT&T POP in the County as well as the County's Operations Center.

- Key methodologies and processes in solution including year-to-year continuous improvement

The SaaS MDM/EDM solution shall include the following key processes:

- User acquires phone and needs access to County resources.
- A request is made for access via an Install/Move/Add/Remove (IMAR) through Contractor's Service Desk.
- User goes to the public apps store and downloads the MDM/EDM application.
- The Contractor team processes the request and gives permissions for allowed systems for the End-User.
- User enrolls into the MDM/EDM system via an End-User guide provided by the Contractor team.
- Any issues are directed to the Service Desk.

Contractor's MDM service shall require a monthly RU and a one-time upfront fee per End-User at the time a new End-User subscribes to the service. The one-time fee includes licensing costs.

Contractor shall participate as dedicated resources supporting upgrades, refresh, and transformational activities related to mobile infrastructure services. Contractor's SMEs shall continue to use Pilot Charter and Solution Design Documents as well as other documents and briefings to convey Contractor's recommendations for County review.

To stay up to date Contractor shall conduct quarterly collaborative reviews of mobile device standards, including hardware and operating systems, for incorporation into the Standards and Procedures Manual for Standard Mobile Devices. Furthermore, the Contractor team shall use the approved Standards and Procedures Manual when developing standards for all mobility infrastructure services that are submitted for approval on a semi-annual basis. Contractor shall conduct quarterly updates to the timeline/roadmap of all mobility infrastructure services hardware and software version life cycles so that responsive time frames and completion dates stay within supported versions of hardware and software.

5.12. Wireless Network Access Services

5.12.1. Process and Procedures

Wireless Network Access Services

- Description of solution to meet the requirements

Contractor shall manage a comprehensive wireless architecture that provides services to County staff and constituents. Contractor's solution shall provide wireless services for managed computing assets on the secured County internal wireless LAN as well constituent and guest assets on a public Wi-Fi infrastructure. This wireless infrastructure shall consist of centralized geo-redundant controllers, wireless access points, various software-based management tools, and security components.

Wireless Infrastructure

Contractor’s two centralized wireless LAN controllers shall provide redundancy and resiliency through high-availability, geo-redundant configurations that leverage diverse facilities (AT&T POP and the County Operations Center). These controllers shall maintain Contractor’s centralized configuration, act as a single point of interface for changes and monitoring, and support a variety of access point models.

Contractor shall maintain and support the 380+ wireless access points throughout the County to provide wireless connectivity for the End-User. The Contractor team has standardized on the Cisco 3702 for wireless access within County facilities, whereas for outdoor areas Contractor has standardized on the Aruba 274/5. Both products shall continue to provide support for legacy connectivity, such as 802.11 A/B/G/N as well as the new 802.11AC standard. This wide range of support shall allow all Wi-Fi capable devices, regardless of age, to obtain connectivity through the County wireless infrastructure.

The Contractor team shall continue to use several software suites to provide visibility deep into the operations, planning, and support of the County’s wireless infrastructure. These tools include management tools, such as Airwave and Cisco Prime Infrastructure, as well as survey tools such as Fluke’s Air Magnet.

Wireless Network Authentication

For County secure wireless, the Contractor team has worked with desktop support services at Contractor to deliver a certificate to all managed devices required to authenticate via EAP–TLS and connect to the County’s secure wireless infrastructure. Contractor shall continue to provide public access in various County locations, such as the libraries, and shall be segregated logically and physically. Additionally, Contractor shall use its next-generation firewall infrastructure, including content filtering functionality, to provide the most robust security available for the wireless infrastructure.

This architecture, coupled with an NAC and PKI initiative, shall serve to further increase the security posture of the wireless infrastructure. By leveraging these capabilities, additional controls shall be enabled, providing seamless access to wireless staff users, while redirecting untrusted/unmanaged assets to a guest access portal via a splash screen, where they can then obtain public network connectivity. This architecture shall support a closed loop system whereby only known, managed assets shall be able to connect to the secure wireless infrastructure, with little to no additional interaction from the users to facilitate this additional security.

- Deployment plan for resources and use of facilities

The local, dedicated LCM team shall provide all design, implementation, support, monitoring, and reporting of all wireless network services.

Core infrastructure for the wireless network shall be housed at the AT&T POP and County Operations Center, which shall provide secure, restricted access. Wireless access points shall be installed upon request in County facilities according to industry and County-approved standards.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor’s engineering team shall work with County’s CTO to evaluate the new and emerging wireless standards and their enterprise readiness. Contractor’s recommendations shall take into account not just the performance of new wireless access points, but also the device standards being used by County End-Users, so that the timing of the investment enables the largest population of users to take advantage of the advancements.

When a recommendation is approved, the Contractor team shall move forward with project management processes, including planning, scheduling, and implementation of the refresh of existing equipment as well as other infrastructure changes.

For equipment issues, the Service Desk and engineering team shall work to identify and remediate the problem.

5.13. Third-Party Network Access Services

5.13.1. Process and Procedures

Third-Party Network Access Services

- Description of solution to meet the requirements

Contractor shall use the existing solution sets in response to expanding business requirements to support third-party access to and from and across the County data network. Overall, three different types of support shall be provided:

- Dedicated leased line connectivity
- IPSec connectivity
- Virtual circuit support.

Each of these solution sets play a vital and specific role in supporting various County business areas. The solution used for access is based on the location of the third-party devices, the type of communication required (system-to-system versus End-User interactive session), the tolerance of bandwidth variations, and latency impacts.

Using the Third-Party Access Request (TPAR) process, Contractor shall determine the required connection types and any details necessary to provision the access. This process shall identify the specific third-party devices, the County resources being accessed, and whether the communications occurs over the internal domain and/or open Internet. This information shall be used to create strict firewall policies so that only the approved devices and resources are accessed for use by the third parties.

Contractor shall provide unified threat management technologies to include intrusion detection and prevention, virus and malware filtering, firewall security policies, monitoring, and reporting for these third-party connections. All data traverses the County's next-generation firewalls to enable full visibility into all data flows up to and including the application level. All data classified as sensitive and above shall be encapsulated in a secure tunnel as it egresses the County network, regardless of its point of origin within the managed network.

Third-party interfaces shall also be included in the LCM team's capacity and performance monitoring services. This approach facilitates reporting on usage and possible impacts to performance resulting from spikes or increases in usage. All access to County resources from third-party users shall be managed via Active Directory and End-User account levels of access.

Contractor shall support and maintain third-party network access models and use cases are as follows:

- **Dedicated Leased Line Connections.** Third-party leased line connections are used to connect the County network to a third-party network via a dedicated transport (i.e., T1, Opt-E-MAN, Opt-E-WAN, and so forth) that is provided by the Third Party. This solution is chosen when throughput must be guaranteed because the dedicated circuit is not impacted by fluctuation in utilization of public Internet circuits. A dedicated circuit also provides the highest level of security in terms of confidentiality, integrity, and availability.

IPSec Connections. IPSec provides a secure tunneled connection over the Internet. It encrypts sensitive data and allows machine-to-machine connectivity for scenarios where automated jobs run connections into or out of the County network without End-User interaction. It also provides access into the County network for authorized systems or users without the need to install specialized VPN software on the remote hosts. Virtual Circuits. The virtual circuit design allows placement of non-County devices onto the County network in a way that keeps them isolated from County assets. All communication to and from County resources is still regulated by firewall policies. Presently, this solution supports users within 55 virtual circuits inside the County domain without exposing the network to risk.

As part of the dedicated team's ongoing efforts to provide continuous improvements to, and enhancements of, all frameworks for which they are responsible, Contractor shall continually look for alternative solutions that benefit the County's voice and data network.

- Deployment plan for resources and use of facilities

The local, dedicated LCM team shall provide all design, implementation, support, monitoring, and reporting of each of the third-party access solutions. All managed hardware in association with such shall be housed at the AT&T POP, which shall provide secure, restricted access as well as fully redundant power. Contractor technical personnel and hardware associated with the County program shall be dedicated to the program.

- Key methodologies and processes in solution including year-to-year continuous improvement

The local, dedicated LCM team shall be embedded in the full life cycle of every third-party access connection—from the initial gathering of requirements, through the design and implementation phases, to managing and monitoring, and even decommissioning when requested. Through customer meetings and security reviews, the team shall evaluate the proper access method so that it is sized appropriately and verifies that all necessary security measures are in place.

Third-party network access options shall be continually evaluated based on County business requirements in addition to current and emerging technologies.

5.14. External DNS Management Services

5.14.1. Process and Procedures

External DNS Management Services

- Description of solution to meet the requirements

The external Domain Name Service (DNS) cloud-based platform, which uses Akamai cloud-based FastDNS service, shall be the basis for Contractor's DNS management service.

The Akamai FastDNS solution shall provide an authoritative DNS service that offloads DNS resolution from the County's infrastructure to the cloud to provide 24x7 DNS availability. It shall be optimized for performance through global distribution and presence and reliability—protecting against DDoS attacks while allowing for additional security through the Domain Name System Security Extensions (DNSSEC) to protect against DNS forgery and manipulation. Contractor shall perform DNS management as required for all of the external-facing County DNS records (A, MX, CName, and so forth) via a web browser that accesses the Luna Control Center. The Luna Control Center is the web-based portal that provides customers with access to—and control of—their Akamai services as well as reporting and monitoring functionality.

Through coordination with the County, Contractor shall fulfill requests to add, move, or change the information published for specific domain name records within the Akamai solution, as well as remove obsolete records to preclude any instances of orphaned or bad records. Although the existing DNS implementations allow a logical separation between the internal and external DNS, Contractor SMEs shall integrate specific elements, as required by the County, subject to essential network security provisions.

Through the use of the Akamai FastDNS service, single points of failure shall be inherently mitigated by the design of the solution. The Contractor team shall regularly evaluate this position throughout the life of the term so that the most cost-effective and technically sound solution is provided to the County.

Also included within Contractor's support activities include the maintenance of a comprehensive roadmap of all external DNS management services required in conjunction with Akamai and the County. This roadmap allows

Contractor to adequately inform its customer and plan time frames and completion dates for any software changes needed to improve service capabilities. As an integral part of these coordinated services, Contractor's SMEs shall facilitate ongoing product and solution strategy planning with Akamai, so Contractor's collaborative roadmaps remain up to date with new and emerging functionality and service changes.

- Deployment plan for resources and use of facilities

The LCM team shall continue to use the Akamai cloud-based resources as an integral part of Contractor's solution. Contractor shall operate and manage the service from its Rancho Bernardo site, where its support personnel shall manage all aspects of the data network to include external DNS support services.

The Contractor team shall leverage some remote resources, such as those from Akamai, and those support activities fall directly within the purview of one or more of Contractor's local SMEs for adherence to the County's requirements.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor staff shall participate in supporting continuous architecture and management activities for the internal and external DNS.

From an external DNS perspective, Contractor shall work to establish new records or remove existing records based on the associated activation or deactivation of new services that tie to an external DNS service.

5.15. IP Address Management Services

5.15.1. Process and Procedures

IP Address Management Services

- Description of solution to meet the requirements

Contractor shall use the BlueCat Proteus Enterprise IPAM v4.0.5-20 Platform as the single user interface providing integrated management of all static and dynamic addresses. Operating within the AT&T POP, this virtualized solution configures and documents changes to the IP address landscape and collects real-time information related to the current IP allocation within the network. A standby platform shall be located within the COC to mitigate against a single point of failure. In turn, the Proteus management platform shall communicate with the BlueCat Adonis appliances that are geo-redundantly located within the COC and the AT&T POP. These appliances shall serve as the policy recipients from Proteus and thereafter monitor, manage, and configure all Dynamic Host Configuration Protocol (DHCP) services within the County's internal network. The Adonis System also relays IP address utilization information back to Proteus for data aggregation, analysis, and presentation, as required.

Due to the inherent capabilities of Proteus, Contractor uses this management platform for a structured approach to IP subnet assignment, to control static IP address use, and to monitor dynamic address allocation. Additionally, Contractor's solution allows IP address data to be collected, analyzed, and organized into the monthly DHCP pool and IP subnet utilization and trending reports for the County. In addition to providing automated discovery of IP addresses, this tool allows Contractor engineers to detect and manage conflicting or duplicate address use quickly so that normal network operations are maintained.

This solution set shall manage and control the network domain using an IPv4 address schema, but it is fully capable of supporting IPv6 when address transformation is required. Contractor shall support the equivalent of 916 Class C address blocks for internal, external, third-party, and public network access through Contractor's data networking services using efficient, fault-tolerant routing so that Contractor's services meet the County-specified service level requirements. The Contractor solution shall be fully and continuously synchronized with the internal

DNS services using the DHCP servers, which provide DHCP clients with the fully qualified domain name and IP addresses for DNS services. Additionally, Proteus provides Active Directory information regarding IP address assignments for System Center Configuration Management (SCCM). Via SCCM, efficient network utilization is maintained by designating Distribution Points (DP) within the domain to service adjacent blocks of IP addresses for system upgrades or patches. In this manner, blocks of IP addresses are automatically directed to the nearest DP, network traffic is localized to the extent possible, and latency is reduced.

- Deployment plan for resources and use of facilities

The LCM solution shall continue to use the County Operations Center and AT&T POP for the reliability and resiliency IPAM services to help the continuity of network in accordance with service level requirements.

Additionally, Contractor shall continue to use the AT&T Trade Street facility to house its local support personnel and manage all aspects of the data network, including IPAM. LCM shall continue utilization of its local team, which has allowed close alignment with the needs of the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor’s SMEs shall continue to use the weekly network architecture meetings and the Enterprise Architecture Forum to notify Contractor’s user community of identified SPOFs or other enhancements and then implement Contractor’s approved solutions. Additionally, Contractor staff shall also continue maintaining a comprehensive roadmap of all IPAM services hardware and software life cycles. This roadmap allows Contractor to adequately inform and plan time frames and completion dates to stay within supported versions of hardware and software.

From an IP addressing perspective, Contractor’s support methodology focuses on four scenarios that require Contractor staff’s intervention to provide the County with timely service:

- **New Site Activation.** Contractor project management personnel are involved in the creation of any new site, and they include IPAM as part of the actively managed project plan. As needed, new block(s) of addresses are allocated for the site, and the recommended DP is also determined.
- **Site Decommissioning.** Contractor project managers are involved in any site decommission, and IPAM is part of the project plan as Contractor recovers existing block(s) of addresses for reuse.
- **Significant site growth projections.** Depending on the scale of growth projected, Contractor project managers shall be involved and include IPAM as a part of the project plan. In contrast, Contractor shall use the IMAR process for smaller projects.
- **Static addresses are required.** To accommodate these requirements, Contractor leverages the existing IMAR process to gain a static IP address, which is issued from a predetermined range for each site defined within the IPAM tool.

5.16. New Site Installation Services

5.16.1. Process and Procedures

New Site Installation Services

- Solution Summary & Rationale – Description of solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

One of the key strategic initiatives for the County has been real estate planning and facility construction for the long term. This has resulted in the design and construction of new, state-of-the-art County sites. Since the beginning of the existing Agreement in 2006, the County has built 87 new locations throughout the region. The majority of these have been Leadership in Energy and Environment (LEED) certified; more than 30 have been awarded the highest level of LEED achievement. AT&T has partnered with the County and Contractor to help plan, engineer, and build IT infrastructure in all of these locations through the new site installation services component of the Agreement.

The current structure of new site installation services categorizes new sites into tiers based on the number of network access, voice, or VoIP jacks resource units to be installed at each location. This has provided the County with the advantage of predictable telecom infrastructure costs when forecasting the overall financials for facility construction. It has had the disadvantage of restricting the County's flexibility in assigning structured cabling work to vendors other than the IT contractor when circumstances warrant.

To meet the County's requirement for the flexibility to engage its own cabling vendor, the Contractor shall provide a solution that includes base services and optional services within the prescribed End-User based tiers that define the site types. This new RU structure shall consist of 5 RU's by site type, with base and optional services within each.

Base services (the fixed component), shall include activities such as pre-field work and requirements gathering, network design, circuit design/provisioning, installation of network hardware and project management that are required regardless of the cabling vendor used.

The optional services (the variable component), shall include all cabling vendor activities as well as contractor project management oversight. These optional components are broken into two work categories to allow the County to select either all or a subset of the cabling work necessary at the new site. The first component within the optional services shall be identified as "Riser Cabling". This component shall include the placement of pathway and rack infrastructure as well as the placement and testing of fiber/copper based cabling runs between MPOE and MDF, and between MDF and IDF rooms/floors. Trenching is not included in this service and shall be the obligation of the County or their contractor to provide. The second optional component of the service shall be identified as "Horizontal Cabling". Included in this service shall be the placement and testing of all wall jacks, patch panels and plenum cabling between the IDF and the workstations or designated end points.

- Should the County elect to move one or both of these optional service components to a vendor of their choice, the resource unit shall be decomposed to provide adequate cost recovery for the remaining New Site services. For example, in a situation where the County were to elect to do their own Horizontal and Riser cabling at a New Site, the cost of these activities shall be deducted from the overall Resource Unit price and Contractor shall execute the base (fixed component) of New Site activities required to establish connection to the County network. Additional clarity on these fixed and optional services can be found in Schedule 16.1-2. Resource and Facility Approach Summary –deployment plan for resources and use of facilities

Resources that Contractor shall utilize for this effort shall include facility project managers and network design and field engineers. They work out of the Trade Street AT&T facility. This team conducts the design and planning function as well as the staging of all equipment used in the construction of the new site. They also interface directly with County personnel at the proposed new site locations.

The structure of the new site installation service requires involvement from the County's General Services organization in those cases where the decision is made to have the structured cabling and other components installed by the County's selected vendor. All new sites do require the County to provide certain components—such as power and air conditioning—that are determined on a project-by-project basis.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's project management team uses standard Project Management Institute (PMI)-based Project Management Methodologies and has successfully used them to bring 87 new sites online for the County. These processes have been tailored to identify all site-specific activities needed to activate IT services at a new location. Contractor's project managers (PMs) actively walk the proposed site with County stakeholders and engineering resources initially and at various points as the project requires. After requirements and the design are fully understood, the project plan, schedule, and task list are developed by project managers —laying out the details of the project as well as capturing internal and external dependencies. Identified as early as possible, dependencies under control of the County or County contractor are managed with a clear understanding of the associated impacts so that they do not become roadblocks to the project's successful completion. At project close, key learnings are identified and documented by the PM for sharing, learning, and continual improvement by the team.

Although external dependencies are not within Contractor's control, Contractor's team routinely focuses on these actions early in each project to mitigate the risk to completion of Contractor's deliverables. An example of this was the Health and Human Services Agency's move into their new Escondido facility. At a critical point in the project, difficulties in obtaining permits from the City of Escondido were identified. The AT&T team noted that these permits were a key dependency in the installation of telecommunications services to the site. To keep the project on schedule AT&T was able to leverage contacts within the City to obtain the necessary paperwork. Working in parallel, the AT&T PM also escalated internally so that AT&T leveraged resources were able to accommodate last-minute schedule changes and so that the County build and move-in schedule was maintained. For this effort, the product team was given the IT Customer Service Award by the County Technology Office.

Another aspect of Contractor's processes include how project RU billing estimates and final billing are determined as follows:

- Project Start: The network design and pricing estimates documented in the initial Scope of Work are based on the County-provided estimate of End-User occupants for the site.
- Project Completion: Upon project completion Contractor shall update the final End-User count in the SOW and present that to the County for project completion sign-off and billing initiation.
- Post Project 6 Months: Contractor shall perform a final true-up assessment 6 months from the County SOW sign-off. If the site End-User count has exceeded the tier limits for the new site RU originally bills, then Contractor shall initiate a billing adjustment.

5.17. Interactive Voice Services

Solution to meet the requirements

Interactive Voice Services are defined as an IVS system which builds on the basic services provided in Voice Services, includes one or more of the following capabilities:

- Call Management Reporting
- Call Recording
- Speech Recognition Application
- County data integration (data dip)
- Wallboard (Physical/Virtual)
- Computer-Telephony Interface (screen pop)
- Work Force Optimization
- Outbound/Predictive Dialer
- Agent Softphone
- Speech Enabled Customer Surveys

Three categories of IVS shall be created. Each shall provide for technical design, infrastructure, licensing, hardware/software maintenance and support and initial End-User training. The categories shall contain the following components:

- **Small IVS** – *shall include Automated Call Distribution (ACD) and/or Auto Attendant (AA) & Call Management System*
    - Automated Call Distribution (ACD)
        - Distributes calls to customer facing agents.
        - Supports the total contact center agent population at all County network locations.
        - Includes trunking infrastructure to support the routing of calls.
        - Can be used as a stand-alone component or in conjunction with an Auto Attendant.
    - Auto Attendant (AA)
        - Supports Touch-tone input to route calls across the County voice network.
        - Includes the professional recordings both English and Spanish menus and prompts.
        - Includes trunking infrastructure to support the routing of calls
        - Can be used as a stand-alone component or in conjunction with an ACD.
    - Call Management System (CMS)
        - Provides reports of contact center agent metrics such as abandoned calls, average talk time etc.
        - Used in conjunction with an ACD to manage contact center performance.
        - CMS is the additive feature which initiates the Small IVS RU category vs. the right-to-use ACD and/or AA capability associated with the Voice RU's.
- **Medium IVS** – *shall include all components from the Small IVS RU category and shall also include:*
    - Automated Call Recording (ACR)
        - Provides for up to 90 days of customer agent recorded calls for both compliance and quality purposes.
    - Virtual Wallboards
        - Provides ACD statistics and messages displayed on contact center agent and supervisor desktops.
    - Agent Softphone
        - Provides IP softphone via a desktop client that provides County contact center agents full functionality whether they are working at their primary County facility, a remote/alternate County site or at home.
- **Large IVS –** *shall include all components from the Small and Medium IVS RU categories and shall also include:*
    - Interactive Voice Response (IVR)

    - Platform for custom applications such as outbound predictive dialing, multi-language support, voice recognition and County data integration.
- Computer-Telephony Interface
    - Customizable interface between IVR and Desktop components to provide database information to a contact center agent when receiving a call from a constituent.
- Short Message Service (SMS)
    - Provides up to 200,000 outbound text messages to specifically defined County client lists.
    - Requires the manual upload of a County file of customer contact information to the hosted platform.
- Work Force Management
    - Centralized platform of work force scheduling, forecasting and adherence of contact center agents.
    - Provides long term strategic forecasting of agent resource requirements based on historical data
    - Integrated with CMS for agent call statistics
- Physical Wallboards
    - Provides ACD statistics and messages displayed on physical monitors in County call centers
    - Includes the controller infrastructure and supporting software to County provided monitors

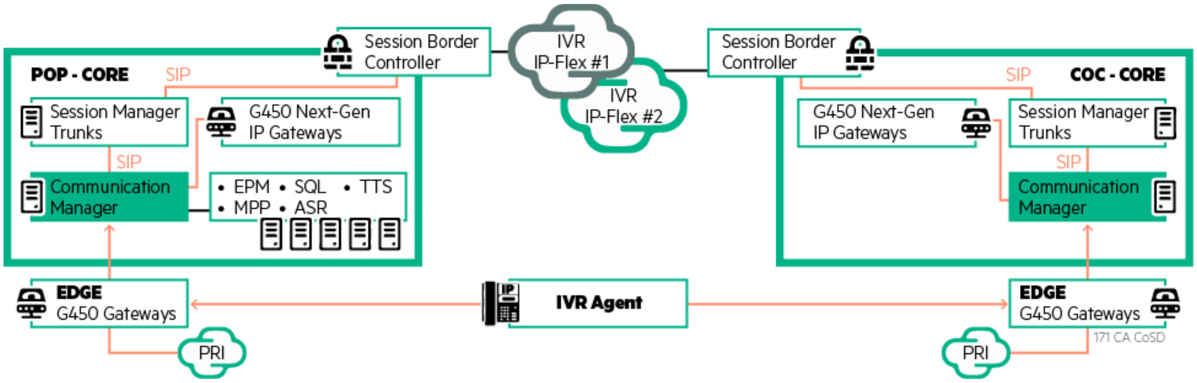
Integrated Voice Response

At the core of the functionality provided under IVS Services is the Integrated Voice Response platform. The IVR infrastructure is built around the Avaya Experience Portal, located at the AT&T POP. This platform provides IVR, self-service, touch-tone as well as speech recognition services for key contact center solutions across the County such as the Department of Animal Services, the Land Use Environmental Group, and various departments within the Health Human Services Agency. This scalable, high-availability infrastructure provides many options for programming and agent integration—allowing customization for any type of constituent-facing contact center service.

The platform shall undergo near-term changes relative to external telephony connectivity as AT&T initiates plans to implement dedicated, fault-tolerant inbound and outbound IP Flex SIP trunks for the County’s IVR infrastructure at the AT&T POP and County Operation Center. This IVR solution shall not impact enterprise voice traffic, allowing business units to conduct high-volume contact center activities, such as outbound dialing campaigns. This new capability shall provide standardized resource unit base from which business units can leverage the platform. This upgrade shall be provided as a Transformation initiative and shall be included in Voice Services as a means to meet relevant scope requirements. Further details of AT&T planned transformation of IVR services is defined in Sections above, Transformation Services, subsection “Initiatives: Voice Services Transformation.”

Over the term of the Agreement, Contractor shall ensure that AT&T develops a transformative roadmap, where proposals shall be developed to increase the redundancy and resiliency of IVR applications, as well as to provide additional feature benefits, such as automated agent call-back and web chat. The figure below presents Avaya’s Experience Portal connectivity.

Avaya’s Experience Portal Connectivity



Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.

- Resource and Facility

The County Operations Center and AT&T POP shall be the primary facility locations for IVS services. Over the life of the term, Contractor shall implement geo redundant systems for key functionality as well as make proposals to introduce new features and functionality. Refresh shall be performed for the systems on a five-year basis.

- Methodology & Key Processes – Key methodologies and processes for year-to-year continuous improvement

As mentioned above, the process for changes and enhancements needs reflect the County's need for flexibility. For minor/basic changes to existing voice applications, County may make these types of changes at no additional cost.

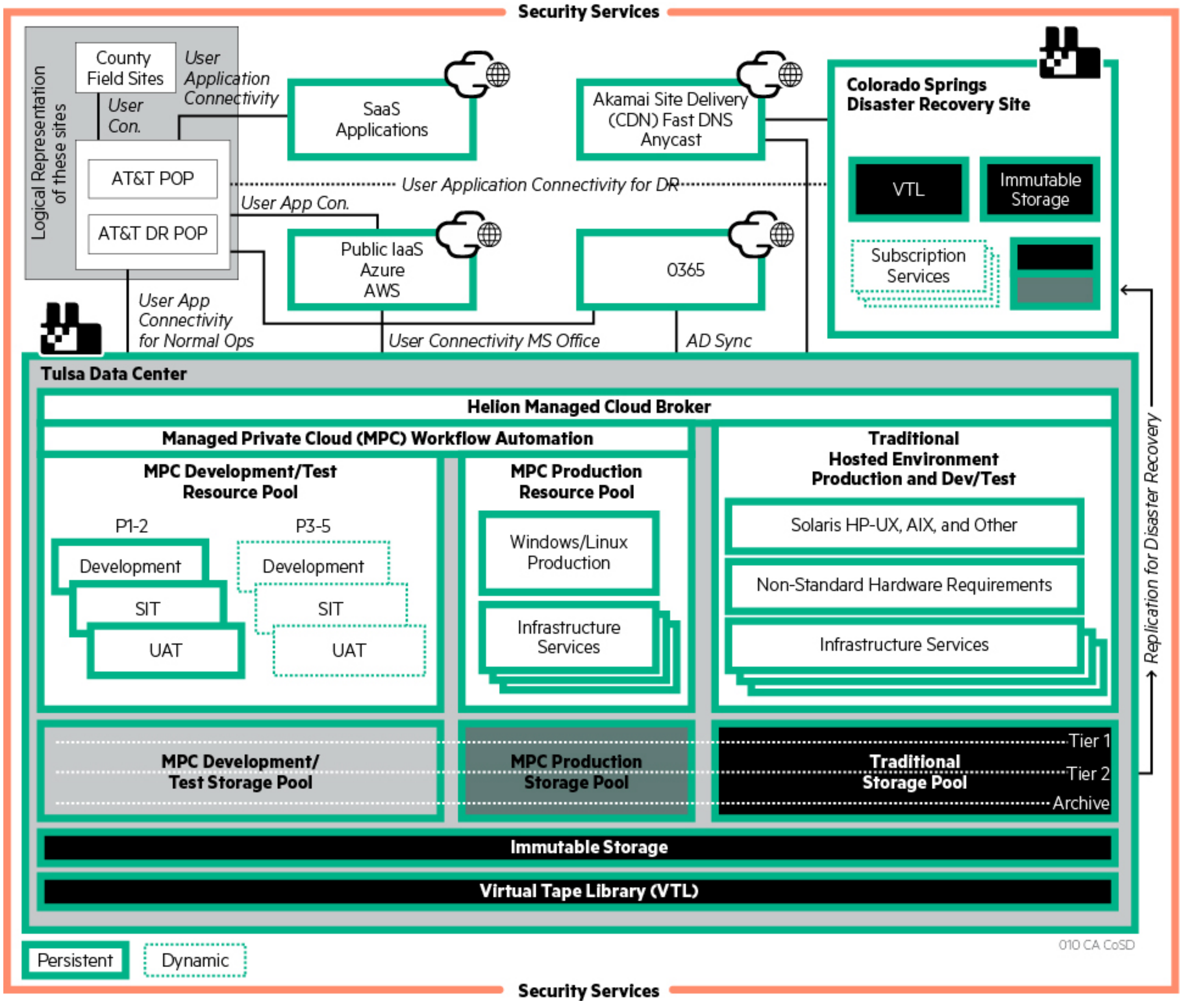
- Additions, changes or deletions to existing call flow/menu prompts
- Additions, changes or deletions to existing routing or transfer points
- Implementation of licenses associated with provided features
- Professional voice recording of changes on basic Auto Attendant and ACD systems

6. Data Center Services

6.1.1. Process and Procedures

Contractor shall provide a data center services framework solution, shown in the figure below, to fully meet the County's needs and facilitate consolidation of applications and infrastructure services into a single Tier 3 production data center in Tulsa, OK. This facility shall be ISO 9001:2008 certified and meet stringent public sector compliance and security requirements.

Contractor data center Services Framework Solution


Security Services
Logical Representation of these sites
County Field Sites
User Application Connectivity
User Con.
AT&T POP
AT&T DR POP
SaaS Applications
Akamai Site Delivery (CDN) Fast DNS Anycast
Colorado Springs Disaster Recovery Site
VTL
Immutable Storage
Subscription Services
User Application Connectivity for DR
User App Con.
Public IaaS Azure AWS
0365
User App Connectivity for Normal Ops
User Connectivity MS Office
AD Sync
Tulsa Data Center
Helion Managed Cloud Broker
Managed Private Cloud (MPC) Workflow Automation
MPC Development/Test Resource Pool
P1-2
P3-5
Development
SIT
UAT
Development
SIT
UAT
MPC Production Resource Pool
Windows/Linux Production
Infrastructure Services
Traditional Hosted Environment Production and Dev/Test
Solaris HP-UX, AIX, and Other
Non-Standard Hardware Requirements
Infrastructure Services
Replication for Disaster Recovery
MPC Development/ Test Storage Pool
MPC Production Storage Pool
Traditional Storage Pool
Tier 1
Tier 2
Archive
Immutable Storage
Virtual Tape Library (VTL)
010 CA CoSD
Persistent
Dynamic
Security Services

Data Center location and solution as it relates to disaster recovery requirements.

The Contractor's Continuity Services center in Colorado Springs, Colorado, shall be the designated disaster recovery (DR) site for the County. Contractor's solution shall incorporate 100% redundancy of infrastructure, provided on a subscription basis, for applications that currently require a DR solution. Production data shall be replicated from Tulsa to the DR site using a dedicated network connection. Contractor's Colorado Springs center shall be a purpose-built, SSAE16-audited data center. The Tier III design shall provide a concurrently maintainable and continually operating facility with infrastructure built with redundant capacity components and multiple independent distribution paths serving the computer equipment.

Contractor's solution shall meet required recovery time objectives (RTOs) of 48 and 72 hours while also eliminating the current dual data center architecture. The Colorado Springs DR site shall have sufficient capacity to support a dedicated environment for an active/active architecture, should the County decide to reinstate it. Contractor shall include in the solution the core network components (Akamai and Global Traffic Management capabilities) to support an active/active architecture.

The DR location and solution shall provide recovery of production midrange and private cloud environments as well as technical assistance for recovery of business processes. In case of a disaster, the production environment shall recover gracefully in Contractor's Colorado Springs data center.

Note that traditional VMWare and MPC environments are handled identically for DR purposes; the Managed Private Cloud is a collection of virtual servers, some of which have DR recovery time objectives, some which do not. The DR environments for the virtuals within the MPC shall be virtual servers that spin up with a copy of the MPC virtuals, for those servers that have designated RTOs in Apps Manager. The Colorado Springs DR site shall have the following features:

- It exceeds Tier 3 data center specifications and:
  - Is on two different power girds
  - Has multiple points of entry for telecom and Internet access
  - Has multiple on-premise power generators that are physically separated—in different rooms with fireproof walls—to make sure that, if there is a fire, Contractor does not lose all of Contractor's generators.
- Colorado Springs provides subscription offerings and Continuity professionals who are trained and certified in Business Continuity disciplines. They shall advance the County's Disaster Recovery strategy and testing methodologies to provide full assurance of application recovery that meets the County's requirements.

Contractor's Rancho Bernardo environment shall use replicated backup sets at the DR site in Colorado Springs to meet remote backup set storage requirements.

Identify and eliminate single point failures with infrastructure and portfolio applications in Data Center Services.

Contractor shall assess redundancy as part of Contractor's design process to avoid single points of failure in the infrastructure and for high-availability (HA) P-1 and P-2 portfolio applications, taking into consideration the criticality of the application or infrastructure element. Contractor shall build quality into the design process by conducting peer reviews so that changes or additions do not create single points of failure.

Contractor shall provide redundant switches in the data center and redundant circuits to the data center. The physical servers shall have redundant connections to the network and to the storage fabric. Physical servers shall be configured with redundant components such as redundant power supplies, which shall be plugged into separate power leads in server racks. Storage arrays shall have redundant components as well, such as redundant disks and power supplies, and shall have the ability to automatically notify Contractor's support teams when an alert is detected on the array. At the application layer, for business-critical applications, Contractor shall incorporate redundant web servers and application servers that are load balanced on the F5s. Databases for business-critical applications shall have replication and/or clustering enabled.

For those applications hosted in the cloud, the Helion Managed Private Cloud (MPC) shall incorporate the tools necessary to continuously monitor server availability across the environment to maintain hardware, upgrade firmware, investigate outages, and perform corrective actions to restore hardware when necessary. Both the MPC and traditional VMware environments shall include spare physical servers that can take over the virtual server load in the event of loss of a physical server in the virtual farm.

The MPC hybrid cloud eliminates single points of failure and meets the service level (SL ID 51) for application availability.

For applications that are unable to meet Service Level 51 without additional redundancy (in both the MPC and traditional environments), Contractor shall add the necessary redundant components upon approval by the County.

The Data Center Services solution for the County shall incorporate the following:

- **Facility Redundancy**: All key components shall be concurrently maintainable, as defined by the Uptime Institute for Tier III facilities, including N+1 data links, power, uninterruptible power supplies (UPS), and cooling as well as redundant network connectivity, power supply, and electrical.
- **IT Architecture Redundancy:** The MPC architecture shall be able to host enterprise-grade workloads that demand high levels of system availability and performance in x86 private clouds. Contractor shall maintain a "system-level" service level objective (SLO) up to 99.95% availability for the entire Infrastructure as a Service (IaaS) stack. This shall include maintaining the availability of the compute; storage; network; security; backup hardware and software, up to and including the operating system (OS); the Cloud Service Automation (CSA) software; and Contractor facilities.

To eliminate server failures, the majority of County traditional hosted applications shall run on VMware virtual machines (VMs). VMware HA shall automatically move and restart VMs on other VMware host servers in the County cluster in case of failure or planned maintenance.

Applications that run in a Solaris operating environment shall use server clustering technology to provide redundancy when needed. Oracle servers requiring high availability shall be deployed in server clusters. If the primary server node fails, services shall automatically fail over to the redundant node. Failover shall also be able to be invoked manually to support a planned outage. More specifically, Contractor shall provide redundancy to the Solaris environment in the following manner:

- Disk
  - OS disk (internal disk): primary/mirror/altboot on three separated disks
  - Application files (external disk array): hardware redundancy
- HBA: At least two host bus adapters (HBAs) per server using either MPXIO or Veritas DMP for multi-pathing
- Networking: At least two physical interfaces for production IP using IP network multi-pathing (IPMP) or link aggregation.
- Server hardware: at least 2 power supplies/ two CPU cores

Private cloud and traditional hosted storage shall use HPE 3PAR enterprise storage designed for cloud environments. The storage shall host OS images, virtual snapshots, and application data. All OS images for virtual machines shall boot from the storage area network (SAN). This architecture shall enable the server image to be disassociated from the physical hardware, allowing the server image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability.

- **Application High Availability**: Contractor shall use the F5 BIG-IP Local Traffic Managers (LTMs) to provide the County application HA by load balancing applications across multiple VMs.

  Contractor shall maintain and support, database clustering tools such as Oracle RAC (e.g., for Oracle IDAM) and SQL Always-On (e.g., for SharePoint 2013) where in use or planned to be in use. The cost of such licenses for database clustering is not included in base services.

- **Disaster Recovery**: To cover higher requirements for redundancy to handle RTO/RPO requirements on mission-critical applications that include P1 Apps – 48 hours with <= 28 hours of data loss and P2 Apps – 72 hours with <= 28 hours of data loss, and services during a declared disaster event, Contractor shall integrate Contractor's Helion Continuity Services delivered through the Colorado Springs DR site.

- **Server Management and Monitoring**: Contractor shall install, manage, and monitor the OS instance and the underlying virtual and physical server. Contractor shall monitor server availability, maintain hardware, upgrade firmware, investigate outages, and perform corrective action to restore hardware when necessary. Contractor shall also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices. Contractor shall use HPE Operations Manager (HPOM) and SiteScope to detect problems and send selected alerts to a centralized management server for specific business-critical applications for County business groups. Thresholds shall be set on events to indicate potential problems, so that support teams can respond to them in time to prevent outage incidents.
- **Special Scenarios: Multi-Facility Presence (active/active facility-level requirements).** In the single data center model, the redundancy components described in the "IT Architecture Redundancy" bullet above shall be applied to applications to provide high availability. For example, the Netmotion environment consists of a single application server and a single database server in each data center. Following the consolidation to Tulsa, this configuration shall be replaced with two load-balanced application servers and two clustered database servers. This provides automated failover within the Tulsa site – a more robust configuration than the manual failover configuration in place today.

If the County wishes to return to a multiple-primary data center model for specific applications, Contractor can locate specific servers at other sites. The location and cost of this approach shall depend on the volume and design required.

Design and support an all virtual infrastructure in the data center.

Contractor shall provide virtualization on a standardized platform to further reduce the number of servers needed.

Approach to Design and Support an All-Virtual Infrastructure: The MPC implementation for the County shall serve as the platform to support an all-virtual environment, providing the bridge from a hybrid environment to an all-virtual environment when feasible. Contractor shall initially retain existing applications in the traditional hosted environment until scheduled for refresh or application upgrade. At that time, Contractor shall collaborate with the County, performing a cost/benefit analysis to determine feasibility to migrate additional applications to the MPC environment. In this analysis, Contractor shall take into consideration items such as level of County hardware investment, timeframe for application retirement, if any, and the level of effort for legacy applications to be re-architected to run in the MPC, if applicable.

MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases. Contractor as part of the solution design shall incorporate the license considerations to manage costs with the expectation of no change in license costs increase based on the virtual solutions.

As part of the Data Center Consolidation transition design process, Contractor shall make all reasonable efforts to optimize County software licensing costs. County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings.

Methodologies to reduce license obligations for server/CPU/core based licenses shall include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment. Contractor shall pursue these methodologies during the design phase of the Data Center Consolidation.

Contractor shall leverage virtualization at the server, storage, and network levels. Virtualization shall separate the applications, data, and network connections from the underlying hardware. Through storage virtualization, the

County shall be able to increase utilization ratios and have greater data tiering flexibility to right-size storage and performance to meet application-specific requirements. With HPE virtualized SDN switches, network provisioning shall be streamlined, making it easier for Contractor to monitor connections.

Contractor shall be familiar with external requirements, such as State or Federal mandates, that can affect the underlying technology demands. Contractor shall collaborate with the County to establish thresholds and project application workloads. Contractor shall combine this information with infrastructure utilization data to create tactical and strategic capacity plans to verify that the County's environment in Tulsa shall accommodate growing and changing business requirements without jeopardizing performance standards.

The MPC infrastructure shall provide the capability to expand capacity quickly due to unforeseen circumstances or emergency situations. This infrastructure shall be supported by Contractor data center professionals who understand the County's business and technical needs. Contractor shall use Contractor's industry-standard software tools to monitor and measure storage capacities and server central processing unit (CPU), memory, disk, and input/output (I/O) utilization and performance on a daily basis.

Contractor shall analyze daily and monthly capacity reporting to identify and address day-to-day capacity constraints. Additionally, Contractor shall analyze capacity trending reports to identify recurring problems that require system upgrades or system refreshes. Contractor shall continue to assess the impact of all changes on the capacity plan and the performance and capacity of all services and resources; tune and optimize the performance; implement County-defined policies; and develop methods to effectively monitor, measure, and report on capacity across the environment. Contractor shall also work with the County departments as they capture forecast demand to produce and maintain a quarterly Capacity Plan that defines planned server system upgrades and refreshes based on growth of existing as well as new application workload. The team shall update the existing capacity plan to reflect each year's forecast. Capacity planning for the County shall encompass the following:

- **Servers** – Capacity management services for servers and mainframes and associated storage shall include monitoring system usage and capacity by analyzing historical resource trends. Contractor shall apply this data during decision-making reviews to assist in formulating environment requirements that meet or exceed future business requirements. Contractor's comprehensive suite of server management and monitoring tools shall monitor the servers against thresholds and alert operations when there is an issue. Metrics shall be captured and run through a data warehouse for trend analysis and capacity planning. Monitoring metrics shall be summarized each day and reported.
- **Planning for Increased Application Usage** – Contractor shall enable performance analysis and availability management to allocate capacity dynamically. Contractor shall use system metrics and statistical reports to gain a clear understanding of overall capacity trends and performance. Contractor and the County shall use this information during decision-making reviews to reshape the compute environment periodically.
- **Network Capacity Planning** – Contractor shall continue to monitor data network usage and performance and generate capacity reports that identify actual and potential network bottlenecks, by establishing capacity benchmarks and by analyzing trends. Such trends shall address the form of overall throughput, percent usage, error rates, and specific performance metrics such as packets per second. Contractor's metrics shall measure both peak and average performance. Contractor shall offer network capacity recommendations for tuning the network to improve efficiency and cost effectiveness.
- **Storage Capacity Planning** – Contractor's storage infrastructure shall support the ability to expand capacity quickly due to unforeseen circumstances or emergency situations. Contractor shall use Contractor's industry-standard software tools to monitor and measure storage capacities, disk, and I/O utilization and performance on a daily basis.

Hyper-converged infrastructure in the delivery of virtual infrastructure.

Contractor shall provide Helion MPC and Helion Managed Cloud Broker (HMCB) to be implemented during the transition period as Contractor builds the County's on-demand Dev/Test and production environment as part of the data center consolidation. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, Contractor shall be able to analyze whether hyperconverged infrastructure shall ultimately yield benefits for the County. If Contractor is able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step would be to move to hyperconverged infrastructure as the data center components come up for refresh. When the County is ready for hyperconvergence, Contractor stands ready to be the County's technology partner to accomplish this objective.

Hybrid cloud integration with data center.

Contractor's in-depth knowledge of the County environment and business objectives enables Contractor to design a hybrid infrastructure strategy that most effectively applies to the County's portfolio of services, accommodates the required workloads, and enables desired business outcomes. Contractor's hybrid approach to enterprise computing combines traditional IT resources for some applications—such as Solaris, HP-UX, AIX, and others—while Windows and Linux applications can be deployed in the cloud. The Contractor's hybrid solution for the County incorporates MPC services with traditionally hosted applications in the Tulsa data center, as described in Application Infrastructure Services.

The HMCB layer enables the County to see all resources —traditional, private cloud, and, in the future (if desired), public cloud such as Amazon Web Services (AWS) and Microsoft Azure—as a unified infrastructure. HMCB shall provide a centralized management layer for traditional and cloud resources managed by Contractor. Contractor's design and architecture shall provide interoperability and integration of tools and common resources (such as storage, network, and security components) with the applications that remain in a traditional hosting environment, enabling smooth transition to hybrid IT.

Contractor shall provide a hybrid model, built using the MPC, customized to the County's requirements, that is scalable and works with the County's infrastructure. Contractor shall optimize the County's applications, as described in the Methodologies and Key Processes section of Application Infrastructure Services to identify which applications are to be in the MPC and which Contractor recommends remain as traditionally hosted.

Additionally, upon integrating hybrid cloud, Contractor shall consider open standards that avoid vendor lock-in as well as architectures with the flexibility to meet the County's changing needs. Contractor shall address the following:

- Continue to support and integrate with the workloads that currently run the business
- Integration must bridge the current applications and workloads with those planned for the future
- Applications differ in how they are designed, hosted, and consumed
- Applications have different infrastructure requirements

Contractor shall use a single management toolset, described in Application Infrastructure, to manage different types of resources. Policy-based placement makes certain Contractor shall deploy workloads to the right infrastructure based on specific business requirements.

Process for physical and virtual servers.

Contractor's hybrid solution shall include Helion MPC services combined with traditional hosted services.

MPC Provisioning: Implementation of HPE's Helion MPC shall enable Contractor to quickly deploy new services where virtual infrastructure is automatically provisioned in hours or less instead of days, upon approval from the County. To provision virtual servers, upon approval by the County, Contractor shall finalize the approved Solution Design Document (SDD) or Confirmation of Server Requirements and shall perform the following tasks for MPC server provisioning:

- **Access the MPC Provisioning Tool** – This provides an intuitive graphical user interface that Contractor shall use to select from a prepopulated catalog of services that Contractor shall define during the MPC build, including provisioning of virtual servers.
- **Browse the Service Catalog** – Using the catalog, Contractor shall browse all predefined offerings and select the primary service desired to initiate the provisioning process.
- **Configure the Requested Service(s)** – Once Contractor has selected a primary service to reflect approved County requirements, the associated selectable options shall be available to Contractor's MPC provisioning team. For provisioning virtual servers, Contractor shall choose the County's required minimum SL, the server name and size including quantity of CPU, RAM, and primary disk size, network connections, server OS, and target resource pool (applications infrastructure, infrastructure, or Dev/Test). Contractor shall then select from a list of predefined templates, which are the County's gold images. Next Contractor shall choose to add-on optional services such as predefined backup and storage choices as required to meet the County's specific workload requirements. Contractor shall then add the item to the cart and repeat this process as needed to configure multiple approved servers simultaneously prior to checkout. Note: Contractor can also reorder or place a request to initiate new services based on prior requests; this streamlines the process.
- **Place the Order** – When the configuration is complete, Contractor shall review and confirm the requested items and confirm the new service(s) or modifications to existing services.
- **Order Fulfillment** – The Contractor initiator receives notification when the automated order fulfillment process is launched, and continues to receive status notifications until provisioning is complete. Contractor shall notify the County once the services or changes are ready.
- **Manage Service Orders** – Notifications shall enable Contractor to track order status in real time. Contractor can also access, monitor, and perform actions on services (such as modifications, cancellations, or deletions), view a detailed list of all orders, and approve requests. Once a service is marked for deletion, a 7-day retention policy is enacted to safeguard the data in case this process needs to be reversed if requested by the County. Additionally, Contractor can track status of servers such as Online, Offline, Transitioning, Reserved, Deploying, Modifying, Modification Failed, Failed, Canceling, Cancellation Failed, Expiring, and Expiration Failed.
- **Manage Services –** For services currently subscribed and running, Contractor can view detailed information about the services and topology as well as the individual components that constitute the overall service delivery. Within this view, Contractor can also request actions such as start, stop, reboot, create or revert snapshot, server resize, and more to manage the County workloads in an expedited manner.

MPC provisioning shall be powered by the following underlying technology and processes:

- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. HPE Server Automation software shall enable Contractor to automatically perform activities such as server discovery, provisioning, patching, configuration management, and script execution to comply with IT configuration standards.
- **Computing Services** – Contractor shall preconfigure the image for automated provisioning. Using administrator privileges, Contractor shall provide OS patching and ongoing maintenance as well as all database and application installations, patching, and ongoing maintenance. Contractor shall monitor system availability and security, and perform root-cause analysis and corrective action of OS; physical and virtual servers; storage, backup and network environment problems; and all other IT Service Management functions.
- **Storage Services –** Contractor's Helion Storage Services enable efficient information management while maintaining the right level of storage from creation to deletion. Contractor shall manage the County's active system data via a storage area network (SAN) platform using tiering technologies to balance cost and performance; this delivers a lower-cost solution, increases business agility, and minimizes risk. Contractor shall virtualize storage resources to increase utilization and provide greater data tiering flexibility.

Contractor shall provision storage infrastructure (hardware, software, and management tools) to store application and database data from the corresponding computing environment. Features include storage performance and capacity planning, monitoring, reporting, asset management, service operations management, and supplier engagement, when necessary.

- **Server Provisioning, Monitoring, and Management** – Contractor shall install this service and configure it to meet County-specific needs based on the following:
  - Resource pool location for capacity provisioning
  - Availability “System Level” end-to-end Service Level for availability
  - Server size (CPU configuration: x-small, small, medium, large, x-large)
  - Server size (GB of RAM: x-small, small, medium, large, x-large)
- **OS Provisioning, Monitoring, and Management** – Contractor shall install a standard build for the Windows and Linux operating systems and monitor availability of the servers and the OS instances up to the point of connection with network demarcation. Upon detection of an availability, capacity, or performance event, Contractor shall investigate the outage and perform corrective action to restore the system. Contractor shall deploy local admin users for Contractor’s Private Cloud Operations OS administration. Contractor’s OS management shall include startup and shutdown, OS patch management, and maintenance job scheduling (at the OS and system level) for private cloud internal management activities.
- **Policy-driven Automated System Provisioning –** Contractor shall automatically provision new cloud infrastructure based on defined policies. New systems are deployed once approved by the County, and Contractor shall periodically advise the County when new OS versions and editions become available.

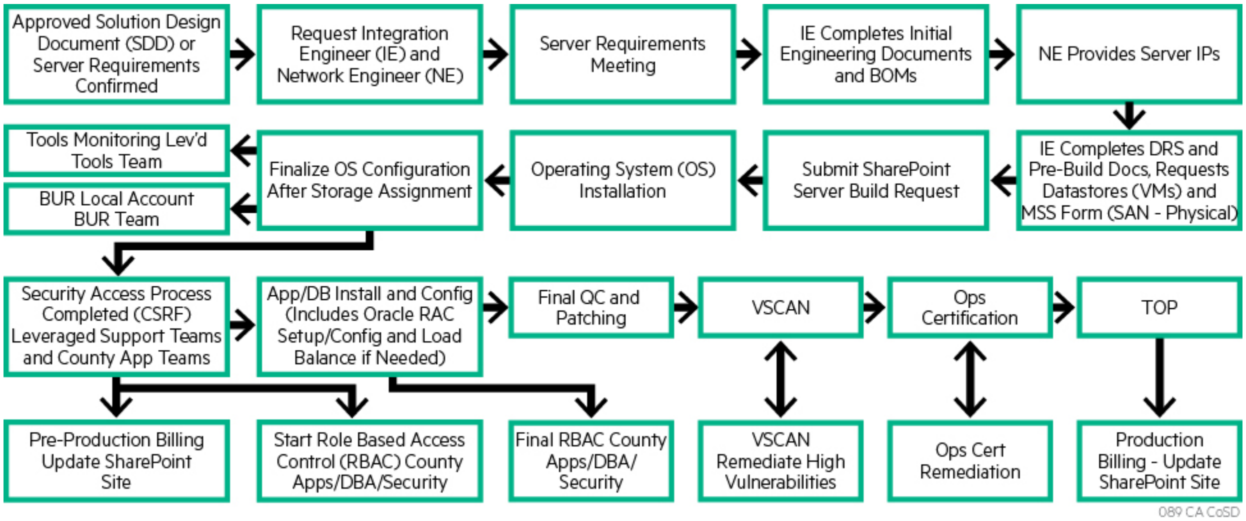
Traditional Provisioning: Using HMCB, Contractor shall perform automated provisioning of VMware servers in the traditional environment. Over the long term, Contractor recommends that all VMware environments within the data center be moved into the MPC and the HMCB provisioning process be used for non-data center servers. The provisioning process for VMware servers in the traditional environment follows the steps above up to the point of layered product installation, at which point Contractor follows the traditional process, described below.

Contractor shall have an established and thoroughly documented process to provision traditional servers that begins when the Contractor server team receives an approved Solution Design Document (SDD) or Confirmation of Server Requirements from the County.

This process shall incorporate all the necessary engineering activities and includes installing the OS, configuring the necessary storage capacity, applying security controls, scanning for vulnerabilities, testing, deployment into the production environment, and finally provided appropriate access to the Applications team to start development or testing as needed.

Adherence to this process shall enable Contractor to meet the County’s Provisioning Service Levels.

Contractor Standard (Traditional) Server Provisioning Process


Approved Solution Design Document (SDD) or Server Requirements Confirmed
Request Integration Engineer (IE) and Network Engineer (NE)
Server Requirements Meeting
IE Completes Initial Engineering Documents and BOMs
NE Provides Server IPs
IE Completes DRS and Pre-Build Docs, Requests Datastores (VMs) and MSS Form (SAN - Physical)
Submit SharePoint Server Build Request
Operating System (OS) Installation
Finalize OS Configuration After Storage Assignment
Tools Monitoring Lev'd Tools Team
BUR Local Account BUR Team
Security Access Process Completed (CSRF) Leveraged Support Teams and County App Teams
App/DB Install and Config (Includes Oracle RAC Setup/Config and Load Balance if Needed)
Final QC and Patching
VSCAN
Ops Certification
TOP
Pre-Production Billing Update SharePoint Site
Start Role Based Access Control (RBAC) County Apps/DBA/Security
Final RBAC County Apps/DBA/ Security
VSCAN Remediate High Vulnerabilities
Ops Cert Remediation
Production Billing - Update SharePoint Site
089 CA CoSD

Physical Server Provisioning shall follow the same process as Traditional Server Provisioning, with the following steps added, following the approval of the SDD:

Workload Placement is a step that engages the Hardware Planning team to determine the floor and rack locations and provide any additional power and cabling, if required.

Network Configuration: Switches and remote access capability are configured.

Hardware Installation: If sufficient hardware is available within the pool of spares, this hardware shall be integrated and installed and connected, once the floor and rack locations are ready.

Procurement shall occur to replenish any spares used by the request; or, for large or specialty hardware orders, this step shall occur before hardware installation.

Storage Configuration: SAN fiber shall be connected and LUN allocations shall be presented to the physical server.

6.5. Security Services

6.5.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall consolidate all services (except mainframe and AS400) from Plano, TX and Tulsa, OK (Tulsa) into a single production data center in Tulsa. The new environment shall incorporate a Managed Private Cloud (MPC) environment for production (upon county approval), development/test (Dev/Test) services, and Break/Fix, and retain the traditional hosting infrastructure for production, Dev/Test and/or Break/Fix that are not compatible. It shall include the deployment of firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) devices, host-based security and full spectrum analysis of all traffic in and out of the Tulsa data center. Contractor shall incorporate robust IT security within the Tulsa data center to meet the specified requirements. Contractor's approach to data center security shall involve disrupting the entire life cycle of an attack, by investing in both layered prevention and detection, and in a network configuration that creates separate security zones.

The Contractor solution shall include:

- **Implementation of Palo Alto next generation firewalls.** These multifunction devices provide firewall services, intrusion prevention and detection services, spyware and antivirus filtering, web content filtering as well as unified threat management capabilities. This solution also provides automated alerting of possible malicious activity and daily threat updates.
- **Network zone restructuring.** The production zones shall be implemented by a combination of network segmentation, device separation, and firewall separation between each of the three zones (Front DMZ, isolation zone, and data center zone). The Dev/Test environment has virtual local area networks (VLANs) representing each of the three zones. The Dev/Test environment shall mimic the production environment. That is, VLANs for Dev/Test shall be located in each of the zones (front DMZ, data center zone and isolation zone). The Dev/Test VLANs shall be segregated from the production VLANs by the firewall and shall not have access to the production VLANs, unless access to specific Services are required (e.g. Active Directory). If a firewall change is required by M&O activity, all labor associated to the firewall change shall be covered under Apps M&O. If the firewall change is required by a new application, it shall be included as part of the project. In addition to eliminating the security risk, it shall provide for more comprehensive application testing. Applications shall be able to test firewall rules earlier in the process and hone during testing. This shall facilitate a cleaner cutover to production.
- **Expansion of ArcSight Security Information and Event Management (SIEM) Services.** All firewalls and IPS sensors, VPN devices, and DHCP appliances in San Diego, Plano, and Tulsa shall be enrolled in SIEM services (log collection, log management, and reporting as well as 24x7 alerting and monitoring services). In addition, Contractor shall include "critical servers" such as domain controllers or servers with data subject to regulatory compliance, such as HIPAA and PCI.
- **Email Security.** With the transition of email to the cloud, email-specific security services shall be provided by the Exchange Online Protection (EOP) capability, which provides comparable security services to the IronPort appliances, such as:
  - Data Loss Prevention (DLP) for email
  - Advanced Threat Protection (ATP)
  - Exchange Online Archiving for Exchange Online
  - Legal Hold
  - Antispam/Antimalware at the mailbox level

- **Distributed Denial of Service (DDOS).** DDOS protection shall include protection at the Internet Service Provider (ISP) layer outside of the County environment, firewall configurations, network configurations, Access Control Lists (ACLs), intrusion prevention system configurations, Web/DNS traffic DDOS protection provided by Akamai, endpoint protection on all windows systems, operating system hardening, browser protection as well as application level protections.
- **Active Directory.** The following components of AD2012 shall be re-engineered as part of the consolidation during transition:
  - Domain controller redundancy standards (rule of three) for the CO domain
  - Flexible single master operation (FSMO) roles failover locations for CO and County domains

- Contractor shall also implement the following tools:
  - **Dell Recovery Manager Active Directory (RMAD)**. RMAD functionality includes the restoration of deleted objects as well as corrupted objects and provides the ability to recover an entire domain or forest in the event either of these is lost or corrupted. RMAD eliminates the need to recreate impacted objects and results in quicker service restoration.

  - **Dell Enterprise Reporter**. Enterprise Reporter provides reports related to Active Directory, which shall provide the County the ability to monitor and manage End-User access and respond to audits.

- Deployment plan for resources and use of facilities

Contractor shall support security services using a combination of resources dedicated to the County and Contractor leveraged resources with specific areas of expertise. These shall include the Contractor CISO, Contractor Security Operations Manager and leads for the various functional areas (threat management, access management, security engineering, risk management among others). The Contractor security teams shall provide the daily support of the various security services and security infrastructure components based on their area of expertise.

Contractor security staff shall be located at the following sites to support the County:

- Rancho Bernardo. Primary location of Contractor staff specifically assigned to support the County. Test environments, training, and video conferencing are housed at this site as well.
- Contractor's Tulsa Data Center – Tulsa, OK – This is the production data center that shall house the majority of the County IT infrastructure, except for that located in San Diego, and delivery of core IT and security services.
- Contractor's Colorado Springs Disaster Recovery (DR) site – Colorado Springs, CO – This location shall be the DR site for the County data center services. It shall provide back up or failover capability for all Tier 1 and Tier 2 applications, core services, and data center security services.
- Contractor's Orlando Data Center – Orlando, FL – This location hosts the SIEM services.

- Key methodologies and processes in solution including year-to-year continuous improvement

Security services for the data center shall be based on the defense-in-depth model developed by the National Security Agency (NSA).

The defense-in-depth model shall also tie to the controls specified in the Risk Management Framework (RMF). As controls are updated in the RMF roadmap, the defense-in-depth mechanisms and associated delivery processes shall be reviewed to identify any potential changes. The potential changes shall be reviewed with the County to determine implementation approach and timing and are added to the security operations roadmap. This roadmap shall contain items to further improve the security posture or maturity of the County from an operational perspective.

All Security hardware and software versions shall be evaluated upon release with consideration for feature benefit and risk. No deviation from standard shall occur without County approval. Patches and updates shall be evaluated as they are made available to determine their applicability to the County environment and shall be deployed immediately as needed.

For cloud based solutions, there are two scenarios for security integration:

1. For cloud services hosted by Contractor, Contractor shall provide end-to-end security implementation, testing, and continuous monitoring.

2. For cloud services not hosted by Contractor, Contractor shall provide, at a minimum, security implementation, testing, and continuous monitoring for all components under Contractor control, such as network and End-User devices.

Contractor shall follow a detailed Security Management Plan tailored to the County that defines the processes used to provide security services and roles and responsibilities for service delivery. It shall describe the technologies and interactions that comprise delivery of security services.

6.6. Mainframe Services

6.6.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide seamless, ongoing operational support to the SA16 LPAR Mainframe and A/S400 in Plano until migration to the new, web-based Integrated Property Tax System (IPTS).

During this time, Contractor shall:

- Be responsible for producing and submitting recommendations for standards on production jobs and Job Control Language (JCL)
- Develop and execute plans to retire the Mainframe and A/S400 upon approval from the County.
- Support Mainframe applications for migration
- Measure Mainframe usage in CPU hours and correlate CPU hours directly to End-User processing for specific applications
- Provide hardware and software utilities to support the Mainframe services
- Be responsible for licensing for all hardware and software used to provide Mainframe services.

As long as the mainframe and A/S400 are live in Plano, Contractor shall support the existing network connectivity that provides End User access, as well as the connectivity to Rancho Bernardo for Managed Print. The DR subscription for the mainframe shall be provided out of Contractor's DR site in Littleton, Massachusetts. Connectivity to Littleton for County End-Users is provided via T1

- Deployment plan for resources and use of facilities

The Contractor team located in Plano shall support the Mainframe until migration to IPTS (mid-range) is complete. Additionally, Contractor staff located in Rancho Bernardo shall support the applications. Following decommissioning of the mainframe, Contractor shall support the IPTS system in Tulsa.

- Key methodologies and in solution including year-to-year continuous improvement

Contractor shall use the following four-step process to decommission the SA16 LPAR Mainframe and AS/400 environments:

- Upon completion of the migration to new applications from the Mainframe and AS/400 environments, Contractor shall decommission the hardware according to standard change management procedures.
- As part of the hardware de-installation process, Contractor shall perform a complete wipe of the disk and tape storage to remove any County specific data. Contractor shall perform a data scrub of all hard drives, permanently removing sensitive data.
- All data stored on tape shall be evaluated for archive requirements. If data archive is required, Contractor shall convert the tape data for access by the new platform. All other data shall be removed (scratched) from the physical media, and either returned to the physical tape scratch pool, or destroyed depending on the condition of the physical media.
- Once the data removal process is complete, Contractor shall remove all hardware from WAN and LAN access. The DASD and tape hardware shall be returned to the Contractor leveraged storage pool for redeployment. The processor environment shall be de-installed and securely disposed.

Following the successful decommission of the mainframe and A/S400, all circuit connectivity to Plano and Littleton for the County shall be decommissioned, and the DR contract cancelled. Any tape media located at the DR site shall be recalled and handled as described in the third bullet above. Contractor shall evaluate the connectivity required for the transmission of interface files, and, if necessary, shall continue to maintain the dedicated circuit.

6.7. Application Infrastructure Services

6.7.1. Process and Procedures

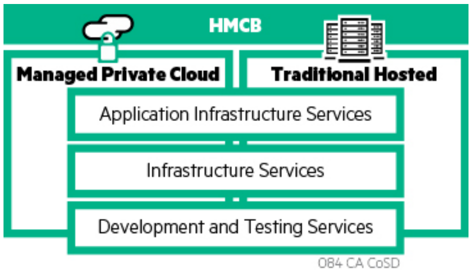
- Description of solution to meet the requirements

To maintain and support County portfolio applications, Contractor shall deploy hardware and software needed to sustain a hybrid computing solution that crosses three framework services, as illustrated in the figure below. Contractor's implementation shall include HPE Helion Managed Cloud Broker solution (HMCB) to provide a high level of automation and orchestration across two pillars: MPC and traditional hosted environments. With HMCB, Contractor shall have the ability to optimize and manage workloads across MPC, traditional hosted VMware, and, in the future (at the County's discretion) other cloud service providers by providing a full service management solution that gives Contractor a single view of the County's IT assets and governance across service management, financial management, operations, and analytics. For applications that are more complex and require greater customization, the traditional hosted environment shall enable Contractor to leverage the County's existing technology investments, and reduce risk by maintaining those environments until and unless they are ready to move. Within these two pillars of the design, each environment shall have its own resource pools for compute, storage, and network, providing the separation of resources required by the County. These resource pools shall be a logical separation. As previously noted, production applications shall not migrate into the MPC during Transition, but shall reside in the traditional VMWare environment until refresh, or such time as Contractor and the County wish to move them.

Contractor shall provide application infrastructure services from the Plano and Tulsa data centers. Contractor shall move compatible platforms in the current application infrastructure from a traditional hosted environment to a more agile MPC. MPC shall support approved versions in accordance to approved County technology standards of Windows and Linux virtual servers.

The pre-defined starting sizes for MPC servers shall be as follows:

Foundation for Application Infrastructure Services



SIZE	CPU ALLOCATION	RAM ALLOCATION
Extra Small	1	2
Small	2	4
Medium	4	8
Large	8	16
Extra Large	8	32

Note that this is only for resource allocation and is unrelated to the billing structure. This range of sizes covers most of the servers in the environment that have a compatible operating system. For servers whose resource requirements are higher (e.g., servers that require 64GB or more RAM), they can still be deployed in MPC as Extra Large, then the resources can be scaled up to meet the application's requirement. Fewer than 10 servers in the environment fall into this category; hence, Contractor did not design additional sizes. If, however, larger resource requirements become more prevalent, additional sizes can be added.

The hybrid environment shall support application infrastructure services, infrastructure services and Dev/Test services (for both Applications M&O and Development and Test projects). The MPC and the traditional hosted infrastructure are sized to accommodate the combined workloads from Plano and Tulsa, and can scale as needed to support the County's needs.

The approximate split of servers between the Traditional and MPC environments is as follows:

Development (Dev/Test + M&O Break/Fix)	271	60

In support of the County's Virtual First strategy, Contractor shall continue to pursue virtualization of as much of the remaining physical environment as possible. When each server comes up for refresh, Contractor shall analyze the rationale for keeping it on a physical server vs migrating to a virtual (and, if possible, migrating it into the cloud environment), and if there is no technical reason a physical server is required, Contractor shall redeploy the server's applications into a virtual server and dispose of the vacated hardware.

MPC Provisioning

As new applications are developed that are targeted to run in the MPC, the Contractor team shall request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team shall then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team shall submit a service request to de-install the MPC infrastructure for that application. The team shall decommission all of the application components and infrastructure resources for the application environment being retired, and release any licenses through Asset and Configuration Management. If the environment is a Dev/Test environment, the request shall specify whether the environment is to be permanently decommissioned or put into cold storage. If the latter applies, the image shall be preserved on the storage area network (SAN) storage and held in an online inventory, but its compute resources released. Otherwise, all resources shall be released.

From a RU billing perspective, RUs are added to billing at the point a production server environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved. If a production application moves from a traditional hosted environment to MPC (as shall be the case during Transition), the old RUs are removed and new ones take effect at the point when the MPC environment becomes available for County use. During Transition, the County shall not be billed for both sets of RUs for any given server. Any move post-Transition from legacy environment to new environment shall be provided at no additional cost to the County, provided that nothing in the legacy environment has changed in a manner that causes additional cost to Contractor.

After Transition is complete, moves between the traditional Dev/Test environment and MPC hosted Dev/Test environment shall not have an impact on billing. Changes to the overall scope of the Development & Test Environment RU shall follow the contract change control process.

For additions to the Dev/Test environment, if the application resource requirements are large, such that its requirements exceed the capacity available (this scenario shall be the exception rather than the rule), Contractor may need to acquire more resources and modify Resource Unit fee accordingly. In most cases, the resources shall be available, and the environments shall be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool shall not trigger a change to RU billing.

For a description of how Contractor shall manage RU billing during Transition, please refer to, Transition Services.

Managed Private Cloud Specifications

The HPE Helion Managed Private Cloud solution shall be built on a predefined, dedicated solution that enables Contractor to rapidly deploy server, storage, and network infrastructure "as service" for the County via a secure, web-based Private Cloud Portal.

The comprehensive private cloud solution shall include HPE hardware and software, professional consulting and implementation services, and ongoing end-to-end management services. The foundation for the solution shall be HPE CloudSystem Foundation. HPE CloudSystem Foundation is a pre-integrated solution that shall enable Contractor to create and manage virtual pools of servers, storage, backup, and networking resources on behalf of the County using a common management layer.

Helion MPC solutions shall leverage CloudSystem Foundation to provide a predefined, prebuilt, highly standardized infrastructure environment. The configurable infrastructure environment shall consist of a set of preconfigured, dedicated hardware building blocks for computing, storage, backup, and connectivity. These building blocks—which can be scaled independently—shall serve as the underlying, enabling infrastructure used to provide the standard Infrastructure-as-a-Service (IaaS). There shall be a base service to which optional services, or building blocks, can be added. Using this approach, Contractor provides an MPC solution that shall be configured to the County requirements, including selection of the mix of virtual machine (VM) sizes and operating system distribution that best map to the County's application profile.

Standard hardware-related services supporting the private cloud environment shall include but not be limited to the following:

- Hardware installation and configuration
- Hardware management
- Capacity management
- Problem monitoring, including proactive hardware support
- Release management
- Patch and system driver management
- Data center facility (floor space, power supply, cooling, wiring)
- Installation of management software

Some of the standard hardware and software products shall be as follows:

- **Server, Storage, and Backup Devices** – MPC uses HPE's Converged Infrastructure including ProLiant Gen9 blades running inside c7000 blade enclosures. Integration with SAN-based storage and backup devices is required in support of an MPC environment. Contractor's private cloud offering uses 3PAR storage options as a configuration standard.
- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO), CSA automatically enables the design and provisioning of infrastructure services in minutes along the End-User-requested

infrastructure configuration. HPE Server Automation software enables Contractor to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with Contractor and County IT configuration standards. CSA also provides the foundation for the cloud service catalog presentation, automation, management, and orchestration.

The Contractor team shall manage the server, storage, backup, and networking resource pools along with System Management Software, such as HPE Server Automation software layers. These products shall help to facilitate the day-to-day operational support for the converged infrastructure-based cloud resource pool. They shall automatically deploy predefined Windows and Linux operating systems into the environment via predefined workflows.

Contractor shall deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. The consistent and reusable private cloud infrastructure shall enable the County to rapidly access the infrastructure when needed. Contractor shall maintain and manage all the software, agents, and monitoring infrastructure of the private cloud.

There are two scenarios of security integration for cloud based solutions:

- In the first scenario, the cloud solution is tightly integrated with Contractor's standard data center security and allows for implementation, testing, and continuous monitoring of controls as required by County policy. For example, the Contractor's Managed Private Cloud allows for this level of integration in which all applicable county policies are implemented.
- In the second scenario, the cloud solution complies with Contractor/County requirements but may not allow for testing and continuous monitoring by Contractor. In this case, the cloud offering is to be vetted so that Third Party assessments take place on a regular basis and that they share the audit reports with Contractor and County. Third Party assessments shall adhere to valid standards such as ISO 27000, ISO 27001, or FedRAMP.

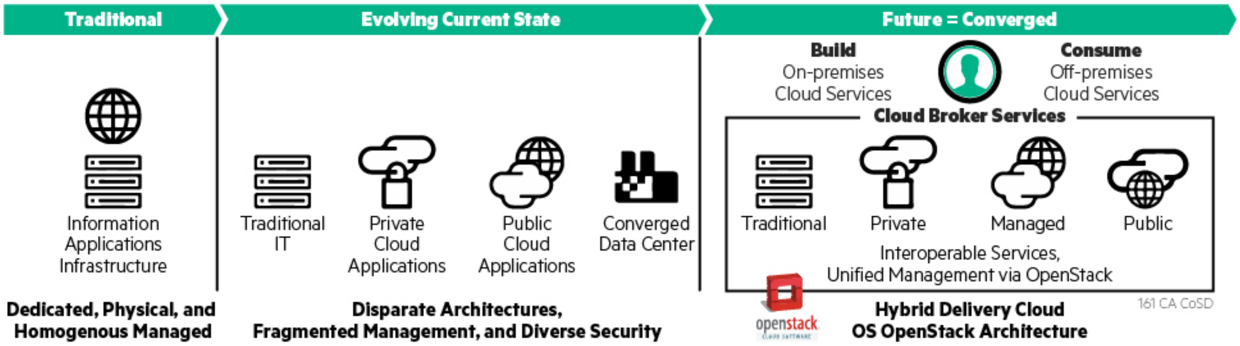
Contractor shall support other key components of the private cloud computing environment, such as CSA and the Private Cloud Portal. Contractor shall support Operations Orchestration, managing the CSA Database, Cloud Controller, and CSA Provider Console, including the following activities:

- Administering the standard Service Request Catalog
- Managing specific CSA settings
- Responding to subscription requests
- Providing lifecycle management of catalog operations
- Supplying standard consumption reports

Implementation of the HPE HMCB shall help Contractor achieve an integrated view of the County's hybrid IT ecosystem and provide the ability to manage VMware-based virtual workloads in the traditional hosted environment both inside and outside of the data center.

With implementation of a hybrid environment in the Tulsa data center, Contractor shall bring application infrastructure improvements throughout the life cycle of an application, whether it is in the MPC or the traditional environment, and whether it resides on a physical server or a virtual host. To improve physical provisioning time, for typical orders of a few servers, Contractor shall keep five (5) spares on hand so that for standard configurations there shall be no wait for procurement. Contractor shall continue to identify opportunities to automate workflows to further improve provisioning of traditional environments to meet or exceed the County's service level requirements. Contractor's complete pre-integrated hybrid cloud solution shall bring to bear data center-wide streamlined service creation, deployment, and monitoring for application workloads, as illustrated in the figure below.

Contractor MPC Standard Building Block and Scale Out Approach to MPC Resources



Contractor shall implement the hybrid delivery architecture shown above under the rightmost arrow (“Future = converged”) to bring these disparate silos together. Once in place, Contractor’s Cloud Broker shall form the basis to create a continual improvement plan and roadmap. This plan shall unify and bring transparency and consistency of governance to these environments, and Contractor shall help the County target future workloads for the right provider and delivery model.

Contractor’s hybrid solution shall provide the following benefits to the County:

- **Faster time to value**. Using the MPC, Contractor shall provide a standard content library with approved County template virtual server (VMs) images that can be provisioned in a matter of hours rather than weeks or months. The standard templates shall allow application solution teams to quickly request web, application and database VMs with preapproved and configured images for the County landscape helping drive the County’s “virtual first” strategy.
- **The right hosting solution for any application**. For applications that require a high level of customization, such as use of non-standard platforms, Contractor’s traditional hosting service provides this solution.
- **High performance application services:** This shall result in better service to end-users, third parties and constituents of the services.
- **HMCB:** Consolidated management and financial governance of traditional, private, and public cloud hosted environments.

- Deployment plan for resources and use of facilities

Contractor shall provide application infrastructure services for the County applications portfolio in Contractor’s Tulsa and Plano data centers, until the consolidation to the Tulsa data center is complete. Contractor shall migrate all workloads from Plano to Tulsa.

Within these environments in Tulsa, the Contractor team, which includes the local team in San Diego, Contractor’s service center in Pontiac, Michigan, and Contractor’s virtual teams of subject matter experts (SMEs), situated throughout the United States, shall manage and operate the application infrastructure services required by these applications.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall use a life cycle approach to support applications infrastructure. Contractor shall follow an application placement methodology in which Contractor shall assess cloud readiness. Contractor shall look at each County application in the production inventory and analyze where that application would best be deployed based on evaluation of the following types of requirements:

- Regulatory requirements

- Performance requirements
- Adherence to infrastructure standards
- Security and confidentiality
- Availability and reliability

When designing the infrastructure to support an application, Contractor shall determine which tiers are required. The tiers shall include the presentation layer, business logic (application) layer, and the back-end (database/transaction) layer. The infrastructure to support any tier can be either MPC or traditional. The County's network zones shall be supported transparently in both environments.

Prior to migration, Contractor shall build out the MPC and upgrade and expand Tulsa's traditional environment to include the required infrastructure for servers, storage and networking components to accommodate the migration of applications into this facility. As part of the consolidation, Contractor shall analyze the application environment and identify the candidate environments to move into the MPC. When this is complete, candidates from the Tulsa environment shall be moved into the MPC to further consolidate and standardize workloads. Upon refresh and subject to County-defined limitations for periodic refresh cycles, Contractor shall continually evaluate additional application workloads to assess the feasibility of moving these to the MPC. Contractor shall analyze items such as County investment, timeframe for application retirement, if any, and the complexity of the development effort for legacy applications to be re-architected in MPC.

For all application infrastructure upgrades, refreshes, and transformational activities that impact portfolio applications, Contractor shall update and maintain AppsManager with information needed in Runbooks. Application infrastructure examples shall be updated DNS, system patches, and sections for outage and notifications, data center and escalation contacts, application interfaces, AD/service accounts and document links, whether provided in the MPC, traditional hosted, or other cloud environments.

Performance Analysis and Improvement

Contractor shall use a variety of methods to analyze performance.

Reactive Performance Management

Contractor shall implement tools to provide early warning alerts to Contractor that shall automatically contact Contractor to look into a situation where some resource or performance metric has passed a threshold point.

Proactive Performance Management

Contractor shall review the trend analytics and reports on capacity and performance on a daily basis.

Netcool and NNMI shall be used to monitor and assess the data center network devices. Performance issues shall be addressed using standard event management (for non-impacting events, such as threshold warnings) or incident management (for End-User-impacting issues) procedures.

Contractor shall review the results of these analyses with the County and make recommendations for County approval.

Performance improvements, in response to either reactive or proactive scenarios, shall include tuning configuration parameters, adding capacity, or making an architecture change such as re-shaping network traffic or moving data to a different storage tier.

Contractor shall also follow the same methodologies and processes to manage the application infrastructure as Contractor does for infrastructure services.

6.8. Infrastructure Services

6.8.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide infrastructure services such hardware, software, network resources and services required for the existence, operation and management of the County IT and telecommunications enterprise, at both Plano and Tulsa until the data center consolidation is complete. These infrastructure services shall provide the foundation that supports County End-Users, third parties, and constituents. The infrastructure services environment shall be comprised of the hardware, software, storage and support services that underpin the operations of the applications and Dev/Test environments, including:

- Server environments that run the supporting tools, including Service Portal, ITSM systems, monitoring, reporting, analysis and alerting systems.
- Infrastructure that provides software distribution and delivery services for mobile, desktop, and data center server environments.
- Local file and print services, distributed throughout County locations.
- Network infrastructure supporting the data center, such as load balancers, WAN Accelerators and global traffic managers (GTMs).
- Background services for applications, such as backups, batch processing and File Transport Protocol (FTP) services.

The servers for infrastructure services shall reside in both the MPC and traditional hosted environment. Over time, Contractor shall work to optimize and standardize this environment as opportunities arise. Servers that support infrastructure services shall receive the same supporting functions (such as performance and capacity management, and backup and restore) as application servers. Contractor shall make sure that no single points of failure exist that could potentially impact the availability of applications or facilities that support County business.

Contractor shall perform comprehensive infrastructure testing for all components in an integrated environment for compute, storage, network, and database in a physical or virtual environment. Contractor shall maintain documentation that identifies all infrastructure services' hardware versions and software version life cycles so that Contractor may adequately plan timeframes and completion dates to stay within supported versions of both hardware and software. Contractor shall also track hardware and software assets to adhere to the County refresh cycle. ESX servers and network components that comprise the MPC shall be refreshed on the same schedule as their traditional hosting/network counterparts.

Contractor shall deliver skilled operations and engineering expertise to manage and monitor the infrastructure services environment, and apply automation to all processes to the greatest extent possible. Contractor shall deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. Contractor shall manage the County's server, storage, backup, and networking resource pools and system management software, to facilitate daily operational support.

Contractor shall manage and maintain the County's server (compute), storage, backup, network, and security environments. Contractor shall follow ITIL-aligned processes to determine critical business impact to component or system failures in infrastructure services, and to continuously analyze, identify and remediate single points of failure in infrastructure services.

Computing Services—Contractor shall install, fully manage, and monitor the operating system (OS) instance and the underlying virtual or physical server. Contractor shall also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices.

In the MPC and traditional hosted environments, Contractor shall preconfigure the OS image for automated provisioning, provide OS patching and ongoing maintenance including performing all software installations, patching, and ongoing maintenance, and monitor system availability and security. Contractor shall perform root-cause analysis and corrective action of OS, physical and virtual servers, storage, backup and network environment problems, and all other IT Service Management functions.

End-User Software Distribution – Contractor shall design, deploy, and maintain software distribution infrastructure and services for End-User computing services and integrate and perform software delivery for County desktop and mobile devices. Contractor's infrastructure services shall include support for devices on the County Public Library private network.

Operating System Software Support—Contractor shall provide a standard build for, then monitor and manage, virtual and physical operating systems such as Microsoft Windows, Red Hat Enterprise Linux and Oracle Solaris. Contractor shall also support other types of UNIX operating systems and VMware as well as other hypervisors.

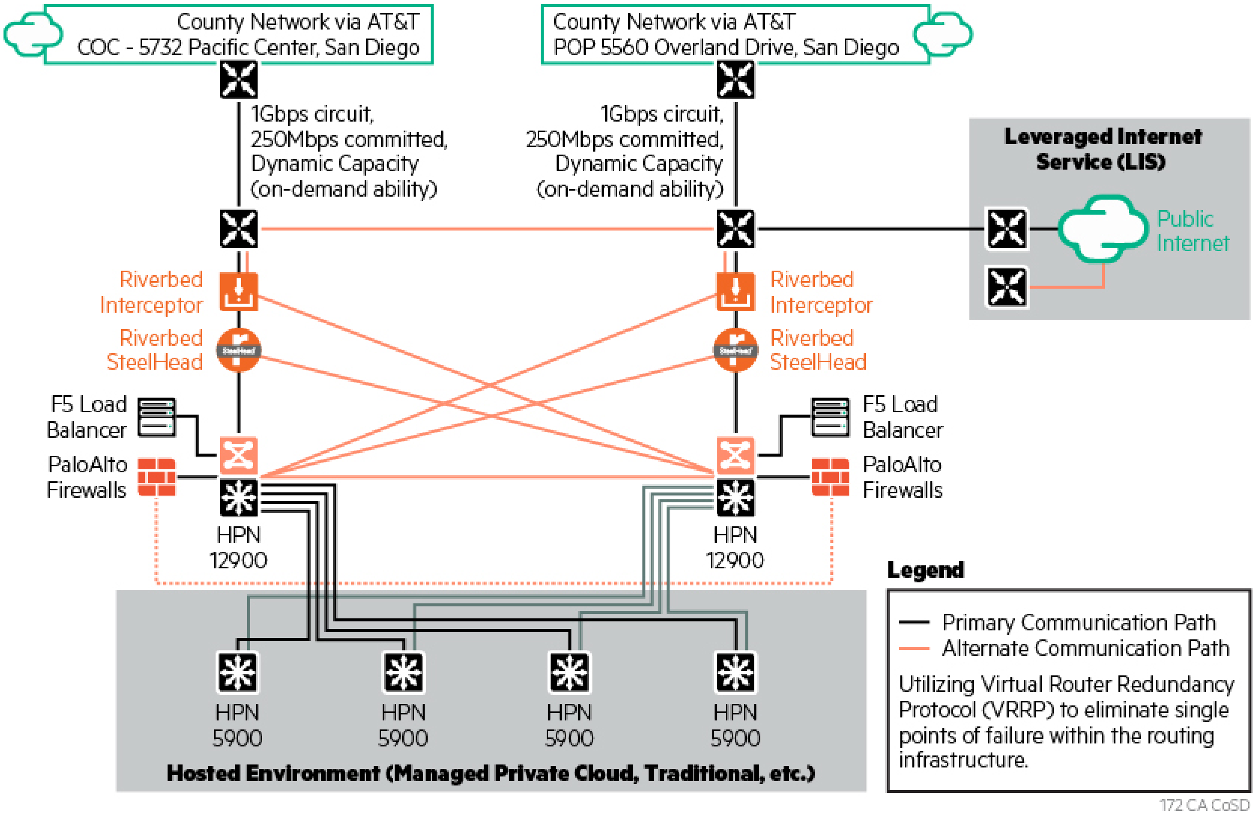
Storage services—Contractor shall use the HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage shall host operating system images, virtual snapshots, and application data. All operating system images for virtual machines shall boot/reboot from the Storage Area Network (SAN). This architecture enables the server image to be disassociated from the physical hardware, allowing the image move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability.

Backup and Restore Services—Backup services for virtual and physical computing services shall provide operating system and filesystem (offline) backup for computing services to enable data restoration after a data loss event. Backups shall be accomplished by copying the specific data to backup media. Contractor shall perform the following:

- Provision backup infrastructure and backup software
- Perform backup management
- Maintain the backup schedule
- Review backup job completion status
- Intervene in the event of backup error
- Store data on disk
- Performs OS, file system, and database restore.

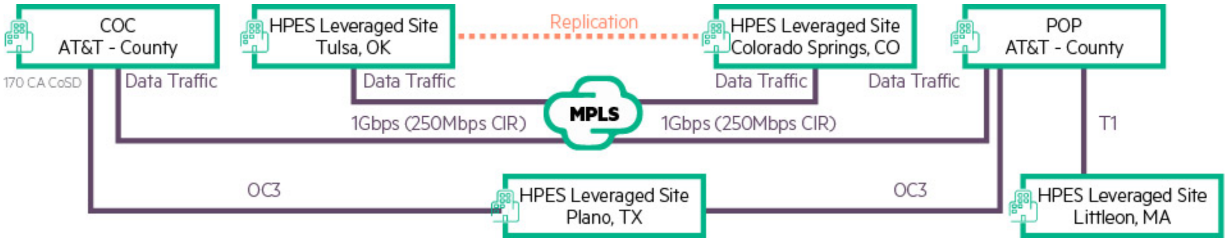
Contractor shall initiate and perform on-demand backups of the County environment. Shortly after the request is submitted, an incremental backup shall begin. For virtual servers, Contractor shall be able to conduct regular snapshot backups of each virtual server instance, with the most recent snapshot being retained for recovery purposes. The snapshot feature shall back up the OS disk and all attached data disks. The figure below illustrates the data center network architecture.

Data Center Network Detail


County Network via AT&T
COC - 5732 Pacific Center, San Diego
County Network via AT&T
POP 5560 Overland Drive, San Diego
1Gbps circuit, 250Mbps committed, Dynamic Capacity (on-demand ability)
1Gbps circuit, 250Mbps committed, Dynamic Capacity (on-demand ability)
Leveraged Internet Service (LIS)
Public Internet
Riverbed Interceptor
Riverbed SteelHead
Riverbed Interceptor
Riverbed SteelHead
F5 Load Balancer
PaloAlto Firewalls
F5 Load Balancer
PaloAlto Firewalls
HPN 12900
HPN 12900
HPN 5900
HPN 5900
HPN 5900
HPN 5900
Hosted Environment (Managed Private Cloud, Traditional, etc.)
Legend
Primary Communication Path
Alternate Communication Path
Utilizing Virtual Router Redundancy Protocol (VRRP) to eliminate single points of failure within the routing infrastructure.
172 CA CoSD

Contractor shall provide a wide area network service construct with diverse paths and entry points into each data center at Contractor's Tulsa, Oklahoma, and Colorado Springs, Colorado, locations. All circuits shall be in an Active configuration to allow operation. Multiprotocol Label Switching (MPLS) circuits with a 250Mbps committed information rate (CIR) shall be used to connect Contractor's data centers to the County's Pacific Center and Overland Drive locations. Each of these circuits shall allow bursting above the CIR to provide on-demand bandwidth increases. Replication shall occur between the two Contractor data centers via a dedicated 10GB circuit. The figure below illustrates this connectivity.

Data Center Connectivity to the County Network



Contractor's WAN and LAN network infrastructure shall deliver multiple, active network paths with 1+1 redundancy at a minimum, whereby multiple components can fail without impacting end-to-end network availability. This enables Contractor to deliver an environment truly capable of targeting 100% availability.

Scalability shall be delivered through the 1+1 active/active construct. Contractor shall use the HPE 12900 and 5900 series switches to provide a high performance, scalable, and open architecture designed for the County to leverage for the next decade. The platform shall be purpose-built for the data center around the principles of modularity, extensibility, and agility.

The network shall be designed and implemented with modularity. This enables Contractor to expand in the future in accordance with the forecast workload. It also simplifies network deployment activities. Contractor shall provide an environment with inherent High Availability capabilities, which is concurrently maintainable, and simple and efficient to operate, reducing the risk of administrative error.

In addition to Contractor's LAN and WAN infrastructure, Contractor shall provide a Leveraged Internet Service (LIS).

Connectivity from the County network to the Plano and Littleton data center, required to remain post-transition to support the mainframe and AS400 environment, is depicted in the diagram above; this connectivity shall remain in place for as long as required to support the mainframe and AS400, and shall be decommissioned once the mainframe and AS400 applications are replaced.

Contractor's LIS shall use circuits from redundant ISP providers, terminated on hardened data center infrastructure to maximize reliability.

LIS shall be offered in monthly subscriptions from 1Mbps to 10Gbps for access to applications and servers hosted within Contractor Data Centers. For implementation during Transition, Contractor shall deploy 50 Mbps, consistent with current traffic requirements in Plano and Tulsa; this shall automatically surge if needed, with no additional charges to the County for surge usage.

Network Management Services—Comprehensive network design and infrastructure management services shall enable provisioning of up to 1024 VLANs per server; monitoring and management of data. Contractor shall implement new network technologies across the enterprise, manage disparate networks, and maintain reliable network performance. Contractor's network management services shall provide a centralized and standardized system that automates network management of End-User data, security, and distributed resources. Contractor shall continuously monitor and maintain all load balancers for optimal operational performance. Contractor shall also deploy and maintain application and network acceleration in the delivery of the Services.

Security Services—Antivirus agents shall automatically be deployed and activated in an automated workflow when a server is deployed. Security policy compliance shall check system configurations against security standards at a predefined scan frequency based on Contractor's security best practices. Contractor shall automatically load policy compliance agents as part of the deployment workflow and maintain and manage the security software, antivirus and policy compliance agents, antivirus definitions, and underlying infrastructure to support the security technology. Contractor shall maintain and provide all infrastructure security components including IPS and firewalls.

Data Center Facilities Services—Contractor shall design all the key supply components (for example, power, air conditioning, and wiring) to be redundant. In addition, Contractor shall control access to the data center to prevent unauthorized entry, and provide a robust infrastructure that provides adequate resistance to damage by the elements.

Costs Included in the Resource Unit (RU)

Hardware - This RU shall include the cost of Load Balancers, Network Accelerators, and Facility charges for infrastructure hosted in the AT&T POP.

Hardware costs (servers and storage) for servers designated as Infrastructure; i.e., servers that run the tools used in providing Framework services, or are otherwise used for a purpose other than to run County business applications shall be included in this RU. Other servers that shall be included in this category are servers that represent a non-variable cost component of another RU; for example, the servers that run the Netmotion and Granicus applications are billed under the Infrastructure Services RU rather than under the RUs specific to those applications because the costs do not vary in linear proportion to volumes. This prevents the possibility of over-billing if volumes grow significantly.

A portion of data center network hardware and circuit cost shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure shall also be included in this RU.

Software - A portion of data center software/tools cost to provide services such as software distribution, performance management, capacity management, and other automation and management functions shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure shall be included in this RU.

Operating system, database and hypervisor software specific to infrastructure servers shall be included in this RU.

Labor - A portion of server, storage and network support labor shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure, as well as the support cost for the network components described in the hardware section above, shall be included in this RU.

- Deployment plan for resources and use of facilities

H Contractor's data center staff in Tulsa, the Contractor local support team in San Diego, and Contractor's virtual team of SMEs, located throughout the continental U.S., shall provide ongoing operations and maintenance of the County's infrastructure.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall operate the Tulsa datacenter in accordance with ISO 27001 and the ITIL framework and best practices. To manage County infrastructure environments, Contractor shall follow ITIL-based service management (event management, and others) best practices.

Contractor shall put in place a process and roadmap to unify and integrate the various providers of services, and develop decision criteria that target workloads with specific characteristics for a specific type of service provider. In addition, continual improvement shall include convergence of tools for a more integrated data center services catalog and more self-service. Contractor shall provide additional self-service capabilities from the Service Portal at the County's pace.

For all infrastructure environments, whether provided in the MPC, traditional hosted, or other cloud environments, Contractor shall provide a robust support service, to include the following processes:

- Hardware installation and configuration
- Hardware and firmware management and support
- OS and layered software product installation and subsequent patching and release management
- Supplier maintenance agreements and coordination of suppliers' activities in support of the applications infrastructure
- Capacity and performance monitoring and management
- Problem monitoring, including proactive hardware support
- Data center facility (floor space, power supply, cooling, wiring) services
- Network integration into the Tulsa data center
- Underpinning services that use the infrastructure services framework (such as directory and domain name management services), described in Section 2.5.

- Refresh of hardware components, at 25% per year for Windows environments and 20% per year for UNIX, Linux, and VMware ESX environments (MPC hardware is included).

These services shall be provided for applications infrastructure, infrastructure services, and development and test services. The work instruction documents for these processes shall be available to the County in the Standards and Procedures Manual.

6.9. Development and Test Services

6.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor's solution for the County's Dev/Test services shall take advantage of the hybrid infrastructure approach described in the previous two sections, employing both the MPC and traditional hosted environments, with resource pools separate from application infrastructure and infrastructure services. This approach shall provide the unified consistent architecture that makes sure the Dev/Test shall provide an accurate picture of how an application's production environment performs. The MPC environment shall be a highly standardized environment with high redundancy and high availability to eliminate single points of failure. Moving to MPC shall provide streamlined server provisioning, enabling Contractor to provision, scale, and de-provision virtual servers in hours instead of days, once approved by the County. It shall also include tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance.

Both the MPC and the traditional hosted infrastructure shall be sized to accommodate the combined workloads from Plano and Tulsa.

The "Dev/Test" RU consists of two logical environments – "Dev/Test" and "Break/Fix." Although there is one Resource Unit for "Dev/Test," the second logical name of "Break/Fix" was added to describe a component of the "Dev/Test" RU for management reporting on utilization and consumption of resources. The logical name "Dev/Test" is used primarily by Applications Development, while the logical name "Break/Fix" is used primarily by the Applications Maintenance and Operations. Details of what is in included in the "Dev/Test" and "Break/Fix" environments are outlined in the appropriate documents.

The MPC environment designed for the County shall provide the following benefits for Dev/Test:

- For Applications maintenance and operations (M&O) Break/Fix environment, dynamic and persistent resources provide a cost-effective solution for certain P1/P2 category applications, Contractor shall keep persistent environments in place, to support rapid test cases, such as performing testing of production fixes in response to incidents. P1/P2 applications shall have persistent Dev/Test environments in the MPC. P1/P2 applications that have been stable for a long time and are not often updated may only need dynamic environments. For these, as well as all P3/P4/P5 environments, Contractor shall take advantage of MPC's elasticity, where Contractor dynamically scales the County's secure, dedicated virtual infrastructure up and down as needed quickly and easily by obtaining and releasing IT computing resources on demand.
- Faster provisioning of hosted application services, and cold storage of dynamic virtual images not in use shall help the County to avoid operational costs and data center footprint associated with paying per-server for idle servers.
- Enhanced scalability and flexibility to adapt to the County's dynamic business demands.
- Security, privacy, and compliance—the MPC infrastructure is 100% dedicated to the County, and Contractor shall protect this behind a highly secure data center firewall. Contractor shall deploy and manage the

technology based on Contractor's extensive security testing practices that meet multi-segment security standards and compliance beginning with FedRAMP Moderate requirements.

- Access to the latest cloud innovations when the County is ready. Contractor shall help the County stay at the forefront of this technology by continuing to offer service and technology enhancements as HPE Labs research and develop next generation cloud systems.
- Integrated with County identity and access management services either through Active Directory or Oracle IDAM.

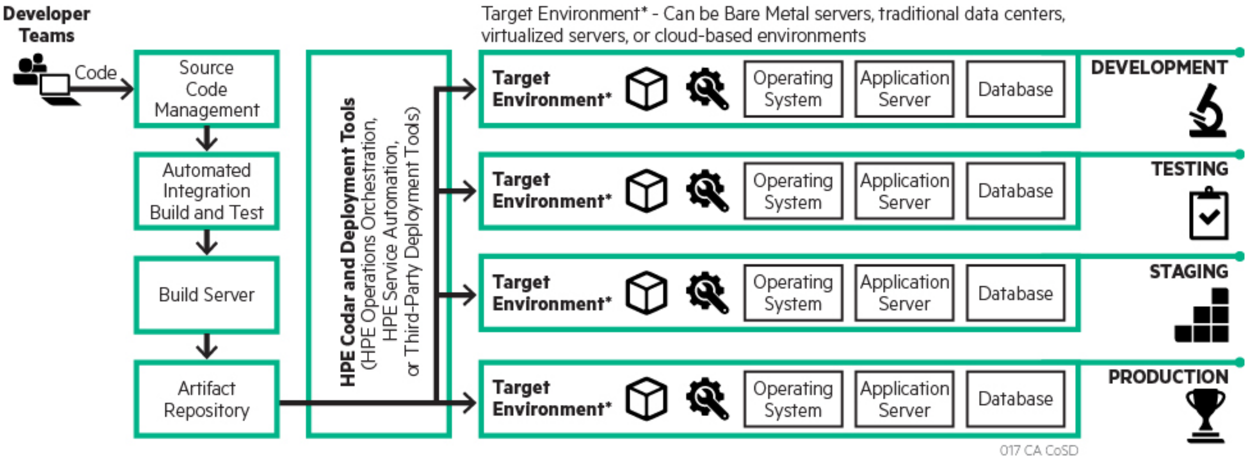
The Dev/Test environment shall be designed to meet County goals for continual improvement and cost effective innovative services to help the County transition to a marketplace of hybrid-provided services governed by Reports 49/50 standards and County IT strategy. Financial governance of the Dev/Test environment shall be through the HMCB and shall provide visibility across the hybrid environment to all Dev/Test resources in MPC and traditional hosted environments as well as public cloud environments.

Contractor's solution shall use the VMware automation built into the HPE Helion Cloud tools.

To further increase the level of automation and improve the Dev/Test environment builds, Contractor shall mature the cloud development, orchestration and delivery tools that shall enable Dev/Test environments to be quickly placed through one-click deployments, automatic rollbacks, and applications promoted across virtual environments. Contractor shall establish modeled environments that shall enable additional consistency through Contractor's automated tools such as HPE Codar and HPE Cloud Automation solution for version-controlled, one-click deployments, rollbacks and promotions.

Employing the same architecture used in application infrastructure services for Dev/Test shall streamline and simplify the migration of applications—from Dev/Test to production. Contractor shall ensure that all individual technical components configured with or added to the services mesh together to achieve the intended results prior to release to the production environment. Contractor shall operate the Dev/Test environment according to all County standards and in close alignment with the production environment. Upon County approval, Contractor shall use the VMware integration capability of the MPC and HMCB to clone production images to the Dev/Test environment.

Automated Tools for Deployment of Environment Models


Developer Teams
Code
Source Code Management
Automated Integration Build and Test
Build Server
Artifact Repository
HPE Codar and Deployment Tools (HPE Operations Orchestration, HPE Service Automation, or Third-Party Deployment Tools)
Target Environment* - Can be Bare Metal servers, traditional data centers, virtualized servers, or cloud-based environments
Target Environment*
Operating System
Application Server
Database
DEVELOPMENT
TESTING
STAGING
PRODUCTION
017 CA CoSD

Contractor's v 4.0 MPC solution is a commercial-release offering and shall be designed as a set of building blocks that can be sized and deployed to fit almost any enterprise's requirements.

Contractor shall provide sufficient SAN capacity in the Dev/Test environment for MPC to store cold virtual machine image files. Contractor shall manage Dev/Test workloads within a SAN-based repository visible to the private cloud and perform tasks such as boot up and shut down of virtual machine images on-demand. Upon the County's request/approval, the tasks shall commence automatically. The Dev/Test environment shall have interfaces enabling connectivity to the production environment as needed to meet business needs. Contractor shall secure these interfaces with VLANs and access control lists. Identity access management services shall be applied across all County environments, including Dev/Test.

Production and non-production virtual servers in the MPC shall never reside on the same physical servers. If the application moves from the development/test phase to production, by making the test VM itself production, then that virtual server shall be moved into the production farm (cluster) when it goes live.

- Deployment plan for resources and use of facilities

The Dev/Test environment is part of the overall hybrid data center architecture and shall reside in the Tulsa data center.

The Rancho Bernardo lab remains available for integration and testing services and proof-of-concept applications or infrastructure that need to be isolated from the production network.

Resources working in the Dev/Test environment shall include Contractor project managers (PMs), developers, and operations staff, as well as designated County stakeholders during End-User testing phases.

- Processes solution including year-to-year continuous improvement

The methodologies and processes used to manage the Dev/Test Service are the same as those described previously in the Infrastructure Services

As described in the Solution Summary section above, Contractor uses the following methodologies:

- IT Strategy and Architecture (ITSA)
- ITIL framework

As a continual improvement initiative, Contractor and the County shall consider adopting development and operations (DevOps) approach to managing development. Contractor shall incorporate DevOps practices of collaboration, source control, deployments through version-controlled models, and system configurations. DevOps shall work together to design and maintain models and configurations in version control from which automated tools can fetch and deploy.

Specific to the Dev/Test environment, the Contractor team shall create new processes for:

- **Automated Release Management** – Using the approach described in the Solution Summary section above
- **Dynamic Image Management –** Used for turning up and down dynamic images and making sure that cold-stored images are reused (as opposed to creating new images every time) and processes for inventorying and removing cold-stored images. For physical servers, images are not dynamic, but if an environment is targeted for turn-down so that its resources may be reused for another project, Contractor shall have processes and scripts to back it up and remove it from active support status during the time while no projects are using its resources.

When a Dev/Test team needs an environment to support a new release, for example, they shall submit a request for requisite resources through the cloud interface or the traditional request process, depending on the resource needed. Upon approval of the request, and determination that sufficient capacity is available to support it, the resources shall be automatically provisioned in the cloud or the traditional VMware environment (or provisioned with task-level automation in the traditional hosting environment) and the requesting team notified of its availability, measured in hours, not months.

6.10. E-Mail Services

6.10.1. Process and Procedures

- Solution to meet the requirements and the rationale

Contractor shall migrate the existing, traditional-hosted Exchange 2010 email to O365 Exchange Online as a transition project.

Contractor shall manage the current Exchange 2010 high availability environment for email service that includes four Exchange servers each in Plano and Tulsa. Contractor's support shall include mailbox management, OWA traffic, ActiveSync, mail relays, GALsync, and RightFax. Contractor shall provide backup and restore functions, and meet special mailbox recovery and journaling requirements. Contractor shall also meet the current retention requirements of 118 days for deleted items and mailboxes and perform backups every other week and retain tapes for 2 weeks before overwriting.

O365 shall fully meet the County's requirements for email services and shall allow the County to take advantage of additional available functionality in a timeframe convenient for the County.

A full discussion of NetBond is provided in the Network Services Framework.

Rationale:

The transition to Exchange Online shall result in the following changes to the existing environment:

- One hybrid exchange server in Tulsa to maintain the local distribution lists
- The RightFax servers in Tulsa shall be connected to redundant local SMTP relays
- Microsoft shall provide email archiving, journaling and e-discovery services.

Contractor shall provide support for email, even after the transition to O365. The Contractor Service Desk shall own the trouble tickets and resolution from start to finish. Contractor and Microsoft shall use Contractor's ticketing system that is devoted to Contractor client support to meet the County's required SLs.

The following table illustrates how Microsoft Exchange Online meets the requirements of the RFP.

Microsoft Exchange Online and Office 365 Features

Requirement	Solution
With respect to licensing, the County has a Microsoft Enterprise Agreement (EA) in place that includes Office 365. The Microsoft EA also includes licensing for the data center Exchange servers.	Contractor's solution covers the County's existing subscription with Microsoft.
Migrate to the current version of Exchange	All MS office productivity applications such as Outlook are continually updated and patched to the most current version. During the migration to Exchange Online, End -Users shall be updated to the latest version of Office 365 Professional Plus. Office 365 Professional Plus shall be installed on all End-User devices as a part of Transition
Migrate to the current version of Outlook to desktops	
Contractor shall ensure high delivery of cloud based E-Mail Services and complete End-User integration.	
Maintain versions of Exchange within 12 months of new releases	
Maintain patch levels of Exchange within 3 months of any new release	

Requirement	Solution
Maintain County retention policies (60 days) without exception	Retention limits can be set across the board or down to an individual mailbox. A County-requested legal hold would be the only exception to the retention policy.
Unlimited Mailbox storage	Contractor shall configure the mailbox to use the archive as the mailbox location to provide unlimited storage.
Unlimited End-User archive storage	
Redundancy built-in to insure minimal down time for E-Mail End-User	MS Office 365 (including Exchange Online) provides 99.95% availability. Their infrastructure is architected with sufficient redundancy and replication to support this level of availability with no data loss due to failures; Contractor provide redundancy of network and surrounding components.
Continuous backup to prevent failure due to data loss	
Contractor shall maintain E-Mail Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.	
Malware and anti-spam protection at the perimeter and within the Outlook client	Exchange Online Protection (EOP) is included in Contractor's solution and provides malware and anti-spam protection at the perimeter and within the server. Malware protection at the desktop is provided by Symantec Endpoint Protection. EOP also provides the following capabilities: - Journaling - E-Discovery - Archiving - Data Loss Prevention Additional information about Exchange Online security is provided below this table.
Immutably preserve or In-Place Hold for End-User data, as requested	
Protection against unsafe attachments at the perimeter and the Outlook client	
Data Loss Prevention implemented per County policy	
E-discovery implemented and used as requested by the County	
Migration of PST files to Exchange archive	The capability to import PSTs in support of eliminating them from the local environment is available. Contractor shall provide migration of End-Users' PSTs
Elimination of PST files from End-User environment	
Implement Outlook Web Access (OWA)	portal.office.com is the Office 365 replacement for OWA—this is provided as part of the implementation during transition. Portal.office.com will only be accessible using County credentials. The process to enforce policy parameters on OWA is described below.
Lockdown OWA to further protect County information	
Mobile aware and productivity included	Microsoft offers a mobile application suite, including Outlook, or users can access portal.office.com via mobile. The same security capabilities apply.
Contractor shall establish and maintain global directory and synchronize E-Mail directories with all County Departments (e.g. Sheriff, District Attorney, SDCERA) or as specified by the County.	Synchronization is accomplished via Azure AD Connect, which Contractor has already implemented for County users. Additional End-User groups shall be added to the synchronization prior to migrating their mailboxes.
Complete migration of all active E-Mail users	Contractor's transition plan shall migrate all active email users
Contractor shall integrate fax capabilities into E-Mail Services for End-Users	Contractor shall integrate the current RightFax solution with Office 365 using a hybrid Exchange server and SMTP relay in the Tulsa Data Center.

Requirement	Solution
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated digital signing to all mailboxes leveraging County PKI platform.	S/MIME is supported and configurable in Office 365.
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated encryption services on all mailboxes based on leveraging the County PKI platform.	Encryption is provided in Office 365 and can be integrated with CoSign and/or the Symantec solution; Contractor shall provide a plan post-migration for County approval.
Contractor shall ensure through continuous review and report that all End-User mailboxes comply with the County's E-Mail retention policy.	Exchange Online provides administrative reporting and auditing that meets this requirement
Contractor shall recommend a plan for County approval, and execute the approved plan to send encrypted E-Mails to E-Mail addresses outside of the County network.	Cloud File Management provides integration into Outlook, which allows transmission of encrypted content to internal or external recipients which require authentication. Exchange Online Data Loss Prevention (DLP) also provides expiration of protected email and content. Cloud File Management has an "I forgot my password" function to enable self-service reset.
Contractor shall recommend a plan for County approval, and execute the approved plan for the ability of external recipients of encrypted E-Mails with access to encrypted content via an authentication.	
Contractor shall enable End-Users an expiration date for sent encrypted E-Mail messages.	
Contractor shall provide self-help password administration for recipients of encrypted E-Mails that permit passwords to be established and reset.	
Contractor shall maintain a timeline/roadmap of all E-Mail Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.	For the Office 365 Pro Plus environment, Microsoft typically releases updates on the second Tuesday of each month to the Internet. Microsoft publishes an Office 365 public roadmap that provides visibility into upcoming releases to the cloud environment. Contractor shall maintain a timeline/roadmap of all email integrated hardware and software that support this schedule and release the Office 365 Pro Plus updates to the County End-User environment according to that schedule. A detailed description of the update process is available on Microsoft TechNet: https://technet.microsoft.com/en-us/library/dn761709.aspx and the public roadmap is available here: http://fasttrack.microsoft.com/roadmap Exchange Online updates are released quarterly. More information about Microsoft's update process for Exchange Online is available at https://technet.microsoft.com/en-us/library/jj907309(v=exchg.160).aspx
Contractor shall provide centralized support and tools for E-Mail Services hosted within the data center or hosted outside the data center.	The Service Desk shall provide the single point of contact for all email support, including Office 365 and all surrounding infrastructure, such as network, firewalls, fax equipment, and other supporting components. Through Contractor's enhanced support

Requirement	Solution
Contractor shall maintain and be responsible for all components needed to provide E-Mail Services (e.g. load balancers, firewalls, IPS).	service, Contractor provides agents co-located with Microsoft support teams to make sure that issues that need to be escalated with them are not simply dispatched but are followed through to completion.
Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to E-Mail Services.	Contractor's Architecture and Engineering team shall provide these services, in coordination with Contractor's Portfolio teams, Microsoft, and Contractor's other suppliers/partners such as AT&T, Symantec, and RightFax.
Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security	

Office 365 Exchange Online Security

Encryption in Exchange Online. Office 365 encrypts data while at rest on their servers and while in transit between End-Users and Office 365.

Data In Transit. Exchange Online supports certificates using Transport Security Layer (TLS) version 1.0 through 1.2, and has recently moved from Secure Hash Algorithm (SHA)-1 certificate support to SHA-2 (Microsoft began deprecating SHA-1 certificate support in June of this year). TLS 1.2 uses Advanced Encryption Standard (AES) with 256-bit length cipher key. Microsoft begins with the strongest cipher key and algorithm and negotiates the proper level with the receiver. There are three types of encryption options with Exchange Online, as follows:

- Office Message Encryption (OME)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Information Rights Management (IRM)

Data-At-Rest. Email data at rest is encrypted using BitLocker Drive Encryption at Microsoft Government Community Cloud Data Centers on hardware using Trusted Platform Module (TPM) version 1.2.

Anti-Malware and Anti-Spam. Users on Exchange Online with Exchange Online protection have their email messages automatically protected against spam and malware. The service has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect the County from spam. Exchange Administrators do not need to set up or maintain the filtering technologies, which are enabled by default; however, Contractor shall make company-specific filtering customizations in the Exchange Admin Center (EAC) or via remote Windows PowerShell, as required.

Spam shall be prevented as follows:

- **Connection filtering:** Checks the reputation of the sender before allowing a message to get through. Contractor is able to create an allow list, or safe sender list, to make sure that users receive every message sent to users from a specific IP address or IP address range. Contractor can also create a list of IP addresses from which to block messages. Since the license includes Advanced Threat Protection (ATP), connection filtering is used by *spoof intelligence* to create allow and block lists of senders who might be trying to spoof the County's domain.
- **Spam filtering:** Checks for message characteristics consistent with spam. Contractor can change what actions to take on messages identified as spam, and choose whether to filter messages written in specific languages,

or sent from specific countries or regions. Contractor can also turn on advanced spam filtering options if the County wants to pursue a more aggressive approach to spam filtering. Additionally, Contractor can configure End-User spam notifications to inform users when messages intended for them were sent to quarantine instead. From these notifications, End-Users can release false positives and allow Contractor to report them to Microsoft for analysis.

Office 365 Exchange Online can also monitor outgoing messages to determine whether they are assuming the characteristics of spam, and allow Contractor to act quickly. Contractor can further enhance spam filtering by creating custom Transport rules based on County policies. For example, Contractor can use Transport rules to set the spam confidence level (SCL) value for messages that match specific conditions.

Malware shall be prevented in the following ways:

- **Layered Defenses Against Malware:** Multiple anti-malware scan engines help protect against both known and unknown threats. These engines include powerful heuristic detection to provide protection even during the early stages of a malware outbreak. This multi-engine approach has been shown to provide significantly more protection than using just one anti-malware engine.
- **Real-time Threat Response:** During some outbreaks, the Microsoft anti-malware team may have enough information about a virus or other form of malware to write sophisticated policy rules that detect the threat even before a definition is available from any of the engines used by the service. These rules are published to the global network every 2 hours to provide the County with an extra layer of protection against attacks.
- **Fast Anti-Malware Definition Deployment:** The Microsoft anti-malware team maintains close relationships with partners who develop anti-malware engines. As a result, the service can receive and integrate malware definitions and patches before they are publicly released. Contractor's connection with these partners often enables Contractor to develop Contractor's own remedies as well. The service checks for updated definitions for all anti-malware engines every hour.

As part of the County's Advanced Threat Protection (ATP) subscription, there are further protections available. ATP helps prevent zero-day malware attacks in the County's email environment. Contractor is able to set up separate policies for ATP to check either links or attachments or both. Each policy can be applied to a specific set of End-Users, at County direction.

ATP aids in both email delivery and Web browsing from links in emails as follows:

- **Email Delivery**: If the safe attachments policy that applies to a particular recipient has an action of "Block," the email shall not be delivered until the attachments can be detonated by the safe attachments technology in EOP. Safe attachments shall launch a unique hypervisor to open the attachment. This can result in a delivery delay of 5 to 30 minutes for each mail evaluated by safe attachments.
- **Web Browsing (Safe Links)**: If a link points to a website recognized as not malicious, *Safe Links* adds very little latency to loading the target page. If the link points to a website recognized as malicious, the End-User is routed to a warning page and has to go through it (if click-through is enabled) to continue on to the site.

Exchange Online is a highly secure email platform with built-in encryption, anti-malware, and anti-spam. Any system is of course only as secure as its weakest link, and typically that link is at the client level. Microsoft has continually enhanced and hardened its mail clients, and Outlook on Windows as well as the Outlook app on mobile platforms is a highly secure portal to the County's email.

Outlook Web Access (OWA) has been Microsoft's web-based email solution for years; because it has been optimized for multiple browsers and versions of HTML, it is perceived as being less secure than other ways to get email. Contractor does not disagree with this perception. If one needs to use OWA, however, there are few methods to make its use more secure. The most secure way to access web-enabled clients is of course multi-factor authentication (MFA), but Contractor acknowledges that MFA is not a preferred approach at the County, so

Contractor is not recommending it. Contractor’s recommendation therefore stands that, to maintain a highly secure email environment across the entire chain, it is most prudent to use Microsoft’s dedicated client apps.

For End-Users who require OWA access, various limitations can be configured using the owamailboxpolicy parameters. For example, OWA on Office 365 Exchange Online can be configured to not allow downloading of any attachment while using OWA. It is configurable in two ways:

- via the GUI (basic on/off)
- via Powershell commands for owamailboxpolicy (which provides more options).

DirectFileAccessOnPublicComputersEnabled	Specifies left-click and other options available for attachments when the End-User has signed in to Outlook Web App from a computer outside of a private or corporate network. If this parameter is set to $true,Open and other options are available. If it’s set to $false, the Open option is disabled.
DirectFileAccessOnPrivateComputersEnabled	
ForceWacViewingFirstOnPublicComputers	Specifies whether an End-User who signed in to Outlook Web App from a computer outside of a private or corporate network can open an Office file directly without first viewing it as a webpage.
ForceWacViewingFirstOnPrivateComputers	
ForceWebReadyDocumentViewingFirstOn PublicComputers	Specifies whether an End-User who has signed in to Outlook Web App can open a document directly without first viewing it as a webpage.
ForceWebReadyDocumentViewingFirstOn PrivateComputers	
WacViewingOnPublicComputersEnabled	Specifies whether an End-User who has signed into Outlook Web App from a computer outside of the corporate network can view supported Office files using Outlook Web App.
WacViewingOnPrivateComputersEnabled	

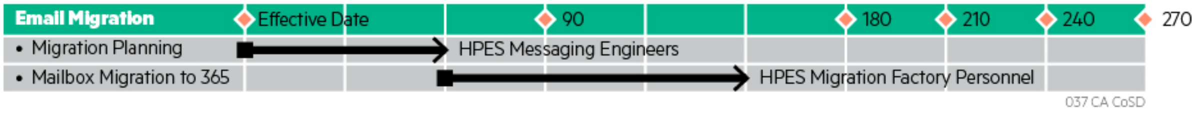
WebReadyDocumentViewingOnPublic ComputersEnabled	
WebReadyDocumentViewingOnPrivate ComputersEnabled	Specifies whether WebReady Document Viewing is enabled when the End-User has signed in from a computer outside of the corporate network.

- Deployment plan for resources and use of facilities

Contractor's approach to O365 deployment is a repeatable process that Contractor developed through numerous successful migrations, including the Contractor corporate email transition. Referred to as the Migration Factory, it is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft cloud. Contractor shall complete the migration virtually, and at the Tulsa data center.

The migration planning process, shown in **Error! Reference source not found.**the figure below which Contractor anticipates to last 60 days, begins at the Contract Effective Date with Contractor's messaging engineers assessing the environment, determining the migration infrastructure need, setting up the temporary infrastructure, and developing a mitigation strategy to address any identified issues. With the migration infrastructure in place, the Migration Factory takes over, moving over email boxes quickly and seamlessly. Contractor expects the migration to occur during an 8 to12 week period.

Email Migration Timeline



Contractor shall provide project management support. Contractor's PM shall guide the process, and County personnel shall be supported through the normal Service Desk for any issues that might arise from an End-User access standpoint.

Contractor shall provide Enhanced Support for Microsoft Office 365. This service is a bridge between Contractor's Standard Service Desk services and the services provided by Microsoft. This is a team that is located in Redmond, WA, with Microsoft. The table below provides a list of the services provided by that team, showing the delineation between Contractor-provided support and support provided by Microsoft. The costs of these services are allocated between the Email RU and the User Data RU (Refer to Transformation Services for a description of this Service).

Contractor and Microsoft Support Responsibilities

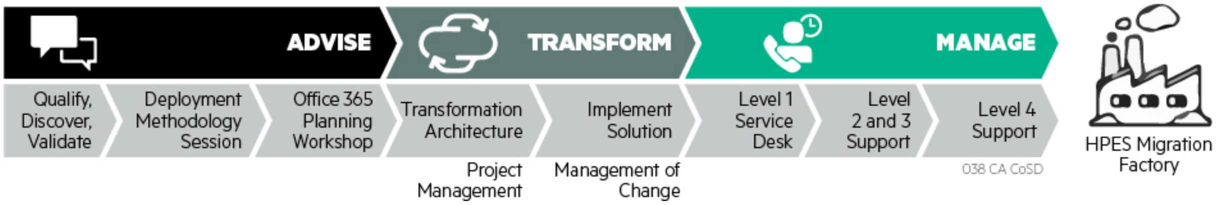
Roles or tasks	Contractor	Microsoft
Contractor and Microsoft Office 365 support team	– Contractor presence in Microsoft Redmond office – Shared document repository – – Knowledge databases, process documents, issue tracking – Weekly team meetings to review tickets, ongoing issues, planned changes, process improvements	
Office 365 service monitoring **Microsoft initiated triage and incident ticket management**	– Action tickets for hardware investigation and repair – Communicate any Office 365 service issues to the County	– Monitor services and platform, hardware, and network – Escalate ticket via case exchange to Contractor
County or Contractor initiated triage and incident ticket management	- Troubleshoot and provide resolution - Escalate via Contractor and Microsoft case exchange - Communicate resolution to the County	– Responsible to troubleshoot and work with Contractor to resolve the incident – Communicate the resolution to Contractor
Post incident time line and summary	Communicate post incident and prior to release of Microsoft Post Incident Response (PIR)	Review time line and summary with Contractor
Post incident response (PIR) and root-cause analysis	– Communicate to the County – Request Microsoft PIR on behalf of the County	– Responsible to develop PIR – Communicate with Contractor

Reporting	– Active and inactive mailboxes – Types of mailbox connections – Mailbox usage and mail activity reports – Mailbox administration activity reports – Mail Security reports – Mailboxes marked for eDiscovery and Litigation Hold – OneDrive for Business sites deployed – OneDrive for Business storage	– Service level availability compliance – Incident reporting – Volume and resource utilization – Post Incident Response and root-cause analysis

- Solution including year-to-year continuous improvement

The O365 Transformation methodology follows Contractor's standard process to advise, transform and manage, illustrated in the figure below. Messaging engineers shall conduct due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel shall use to move from Exchange 2010 to Exchange Online. As groups are migrated, Contractor shall move into the manage phase, providing support for the entire Office 365 suite from Contractor's Service Desk to Contractor's Contractor/Microsoft co-located support group in Redmond.

Contractor Transformation Methodology



6.11. Unified Communications Infrastructure Services

6.11.1. Process and Procedures

- Description of solution to meet the requirements

With the transition to O365, the vast majority of the County's email shall come from Microsoft's Government Community Cloud, as well as the Lync/Skype for Business infrastructure.

While most End-User experience with UC is local, the underlying functionality shall be delivered from the Microsoft Government Community Cloud. Contractor shall continue to support Avaya phones at the desk and from the AT&T POP in San Diego.

Hosting UC in the cloud is the most-cost effective and technically feasible approach as this architecture is designed for Cloud Delivery.

- Deployment plan for resources and use of facilities

Aside from a single hybrid Exchange server and an email relay in the Tulsa data center, almost all of the data center Services infrastructure for Unified Communications shall be in Microsoft's Government Community Cloud.

Some features of the Government Community Cloud shall be as follows:

- The County's content is stored within the U.S.
- Access to County content is restricted to screened Microsoft personnel.
- Office 365 Government complies with certifications and accreditations that are required for U.S. Public Sector (USPS) customers, such as FedRAMP Moderate.

Lync/SfB functionality shall be, by the end of transition, on O365 Exchange Online also.

6.12. Storage Services

6.12.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide storage capacity to support Tier 1, Tier 2, and all dependent applications in the Tulsa data center using a dedicated SAN. The 3PAR P20000 shall have a 5.6TB of Solid State Disk (SSD) storage for 3PAR metadata. Service storage tiers shall be provided as follows:

- Tier 1 storage in the Tulsa data center shall be configured using low cost 10,000 RPM drives, blended with 9.6 TB of flash storage, that are thickly provisioned and shall provide higher performance at a lower cost than the current 3PAR with 15,000 RPM drives.
- Storage for Tier 2 applications, shall use 10,000 RPM disk drives when thinly provisioned or combined with 7200 RPM disk drives.
- Contractor shall also use 7200 RPM disk drives for archive storage that includes low performance, End-User replicated or infrastructure services.

Contractor shall use the SAN 3PAR array to develop, install, and maintain Wintel and UNIX application infrastructure storage. In some cases, direct attached storage may be required for ongoing service support. Contractor shall work with the County to develop plans to migrate all services requiring storage to the SAN storage solution.

Contractor shall refresh the EMC Centera for the immutable storage tier in the Tulsa data center and at the DR site. The immutable storage shall be replicated from the Tulsa data center to the DR site to ensure a copy of the documents on immutable storage are available during a DR event.

At the document processing center (DPC) Tier, Contractor shall use a storage cache for scanned paper documents that shall be transferred to immutable storage in Tulsa.

Rationale: Tiering Level.

The storage solution provided is a 3PAR 20000 with the same storage tiers provided from 10,000 RPM drives and 7,200 RPM instead of the 15,000 RPM and 7,200 RPM drives. This is possible because the new 3PAR 20000 uses an internal infrastructure to achieve better performance using 10,000 RPM drives. The architecture features the HPE 3PAR Gen5 Thin Express ASIC for hardware accelerated thin technologies, including inline deduplication and 5.6TB of flash storage. Using 10,000 RPM drives provides a lower price per GB of storage at a higher level of performance.

The 3PAR 20000 solution with SSD disk drives, 10,000 RPM disk drives, and 7200 RPM disk drives was selected to provide better performance with lower cost disk drives than the current 3PAR P10000 with 15,000 RPM and 7200 RPM drives.

The current 3PAR P10000 storage is using a maximum throughput of only 2450 KBs per second, and the 3PAR 20000 with 10,000 RPM drives is able to provide throughput of 2438 MBs per second—a rate that is nearly 1,000 times greater than the Country is using in their current storage solution. Providing more than 1,000 times the performance than the Country is using would not be money well spent, and providing 10,000 RPM drives shall more than meet the performance that the County requires.

The figures below were generated from the County's recent storage activity. Performance data from the two current 3PARs were used to simulate the expected performance of the new frame. The current Tulsa and Plano 3PAR P10000 reached a peak of ~2450 KBs per second, while the 3PAR 20000 10000 RPM drive storage is capable of 2438 MBs per second. The 3PAR 20000 is the latest innovation in enterprise storage from HPE. It is the evolution of the time-tested 3PAR storage, so there is little risk to the County by refreshing this storage. Primary data (all 3PAR-based tiers) is replicated to the DR site for applications requiring a 48-hour RTO. **Error! Reference source not found.** summarizes performance of 3PAR 20000 with 10000 RMP drives.

Performance Summary 3PAR 20000 with 10000 RMP Drives

Drives	Quantity	Model	RAID	Workload	I/O size	R/W	MB/S	IOPs
SAS	608	1.2TB SAS 10K SFF	RAID5 (7+1)	Random	32K	60% Read	2,438	30
SSD	32	400GB SSD SFF	RAID5 (3+1)	Random	32K	50% Read	4,712	150,796

EMC Centera was chosen for immutable storage. EMC professional services shall be used to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

Contractor selected this storage solution because it delivers a cost effective approach through the use of different types of storage media aligned to meet the criticality of the applications being stored. In combination with the MPC storage capabilities, the storage capacity shall provide the flexibility desired by the County because it can be allocated as needed to meet changing requirements.

- Deployment plan for resources and use of facilities

With consolidation of the data centers to Tulsa, storage shall be provided at Tulsa and at the DR site in Colorado Springs. Contractor shall provide storage administrators in Tulsa and a supplemental staff in San Diego to support all County locations. All of these sites shall be access controlled to restrict physical access only to people who need it.

Contractor's San Diego storage team shall have overall storage management responsibilities as the central storage management point for the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall follow established and proven methodologies and key process in all aspects of operations and maintenance (O&M) support, and Contractor shall fully support the County as described below.

- Contractor shall utilize an ITIL framework, Contractor's proven SOPs, industry standard best practices and County policies, processes and procedures to provide storage and innovative, proactive, and responsive O&M.

- Work with the County to develop plans to migrate service from direct attached storage to SAN storage.
- Refresh, support, and manage DPC storage.
- Work with the County to make sure application infrastructure services Contractor SAN storage.
- Support the traditional data center and MPC in Tulsa using the same SAN 3PAR to provide a centralized storage services solution managed by a single SAN administration team.
- Provide usable capacity reports to the County not to include replicated, backup, or DR data storage.
- Provide 20% year-over-year storage growth for 5 years to accommodate the County's business growth.
- Produce storage services reports by storage tier to the Business Group, department, and End-User levels.
- Provide OneDrive for Business for End-User unstructured data storage on Microsoft's Government Community Cloud. User can log into the OneDrive for Business portal to monitor and self-manage OneDrive storage. Contractor shall work with the County to provide self-service reporting and self-service management in other areas of storage services. Initially this shall be access to regular monthly storage reports via the Service Portal, but if desired, Contractor can expand this to include ad-hoc reporting.
- Work with the County to lower the cost of storage.
- Continually evaluate, evolve, and deliver plans to reduce data loss for storage services.
- Produce and submit recommendations on storage services architecture.
- Produce and submit plans on shared storage services consolidation and application server migration to shared storage services environment annually.
- Produce and submit storage services policies and procedures.
- Produce and submit storage services reporting policies and procedures.
- Produce and submit storage services refresh plan annually.
- Produce and submit plans for meeting storage demands.
- Produce recommendations for process improvement in backup and recovery for storage services assets.
- Recommend and submit recovery policies/procedures for storage services assets.
- Produce and submit recommendation on capacity management.
- Produce and submit plans to add storage.
- Plan and schedule all storage-related software/driver/microcode patching and upgrades.
- Design and implement recovery processes based on approved policies/procedures.
- Design and implement storage services management processes based on approved policies and procedures.
- Implement storage services reporting.
- Design and implement storage consolidation based on approved recommendations.
- Deploy, manage, communicate, and report on activities related to storage service refresh
- Design and implement storage services provisioning and allocation processes based on approved policies
- Design and implement capacity management
- Implement approved Storage services policies and procedures
- Implement necessary physical and logical security to protect the County's data (through access controls, storage network, and host-based allocation controls, SAN zoning and host/array-level logical unit [LUN] masking).
- Provide support, including break-fix, for all storage services assets.
- Manage and affect the appropriate resolution of Incident events until the operation of the storage is returned to normal by following customized procedures as well as resolving Incidents upon an automated or manual detection of an event related to storage components
- Manage and support the storage services,
- Produce and submit monthly storage services reports,
- Support storage services refresh,
- Perform and support media management activities for storage services
- Manage and support the media requests
- Provide data storage services (such as RAID groups, storage pools, LUNs, presenting— masking and zoning, reclamation, optimization—tiers, deduplication, thin provisioning, among others)
- Perform tapes mounts as required.
- Perform special tape shipments as requested.

- Provide options for on-premise and offsite data backup storage.
- Provide backup and restore options such as single End-User restores.
- Load and manage third-party media as required.
- Prepare and manage media for use by microfiche service.
- Manage and perform file transfers and other data movement activities related to break/fix or consolidation of storage services assets.
- Perform data backups of storage services per approved policies and procedures.
- Perform recovery processes on storage services assets.
- Perform storage utilization management.
- Manage and maintain all storage services assets and services.
- Produce and submit storage services management reports,

Classification of County data to match required storage tiers.

Classification can imply the County's standard sensitivity classification structure: Public, Sensitive, and Confidential; however, classification can also be extended to permit very granular categorization to support specific policies.

Contractor shall tag documents as they are ingested using a technology-oriented approach to analyze and auto-classify the data.

Contractor's structured four-step process for data classification shall include the following:

- **Understanding the Landscape** – The process begins by gaining insight and understanding of the legacy and "dark data" landscapes. Contractor defines dark data as information assets collected as normal business activity, but these are generally not used for other purposes. Contractor then creates a Solution Roadmap illustrating the go-forward plan and Return on Investment (ROI) for the organization. For the County, Contractor shall accomplish this by sampling approximately 1 TB of data currently residing on the County's existing file share environments. The assessment shall showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made around data management, archiving, retention, and retirement.
- **Develop data categories** – Using automated tools and common categories, Contractor develops a set of categories specific to the County such as Public, Sensitive, and Confidential. Contractor selects a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of these draft categories shall not affect documents in production systems.
- **Refine and Test** – To determine the relevance of the categories to enterprise documents, refining a category is done by adjusting the weighting of a term, the selection threshold, or by adding a field text. These activities can be done individually or in combination. A category can be published, making it available for use in automated policy execution against content managed by the tool suite.
- **Auto-Classification (requires optional Transformation project)** – Once unstructured data is categorized; Contractor applies policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, Contractor can automate policy application and govern all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating unstructured data across repositories helps to minimize storage costs and reduce discovery times.

Use of Tools

Contractor shall use tools native to 3PAR that are included in the software of the storage devices.

The 3PAR provided in this solution shall be capable of creating thinly provisioned volumes. The Contractor storage team shall be well-versed in managing these volumes, including close monitoring of volume growth that results in having storage available when needed. Traditional provisioning of storage volumes generally results in large amounts of unused storage that has already been dedicated to a host. Thin provisioning allows for over allocation of the 3PAR storage array and reduces the County's cost by delaying physical storage increases.

The 3PAR shall also have auto tiering capabilities with flexible configuration rules that allow for internal automatic migration, lightly accessed data on high performance, high cost storage to more cost effective, lower performing storage when the need for high performance storage is not warranted, based on the auto tiering configuration. The auto tiering configuration is flexible and allows Contractor to adjust the data migration criteria to rebalance data and free up higher performance storage as needed.

HPE 3PAR System Reporter Software shall be used to automatically collect data on a number of different object data points in the background. The Storage Administrator shall use the 3PAR StoreServ Management Console (SSMC) or the 3PAR Command Line Interface (CLI) to display and report on collected data from an array. Using the SSMC, graphical reports are available for the following metrics.

- Historical data (Performance, Histogram, Capacity)

- Real time data (Performance)

HPE 3PAR System Reporter is a feature-rich analytical engine, which helps Contractor interpret and respond to collected performance data and make sure the Portfolio Applications are performing optimally in the environment.

6.13. Backup and Recovery Services

6.13.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall continue to create backup schedules and policies for the County's data. Contractor shall monitor the backup infrastructure, follow the change management process, facilitate backup completion, and restore backup data on a consistent basis by performing backup restore tests at least once per quarter. The BUR solution shall be adaptable to a non-disruptive transition of services.

Contractor shall provide the current BUR services at the Plano and Tulsa data centers and at the County's sites.

In preparation for the data center consolidation, Contractor shall provide planning support to the County and minimize disruption as workloads and technologies evolve while providing O&M support during transition without interruption.

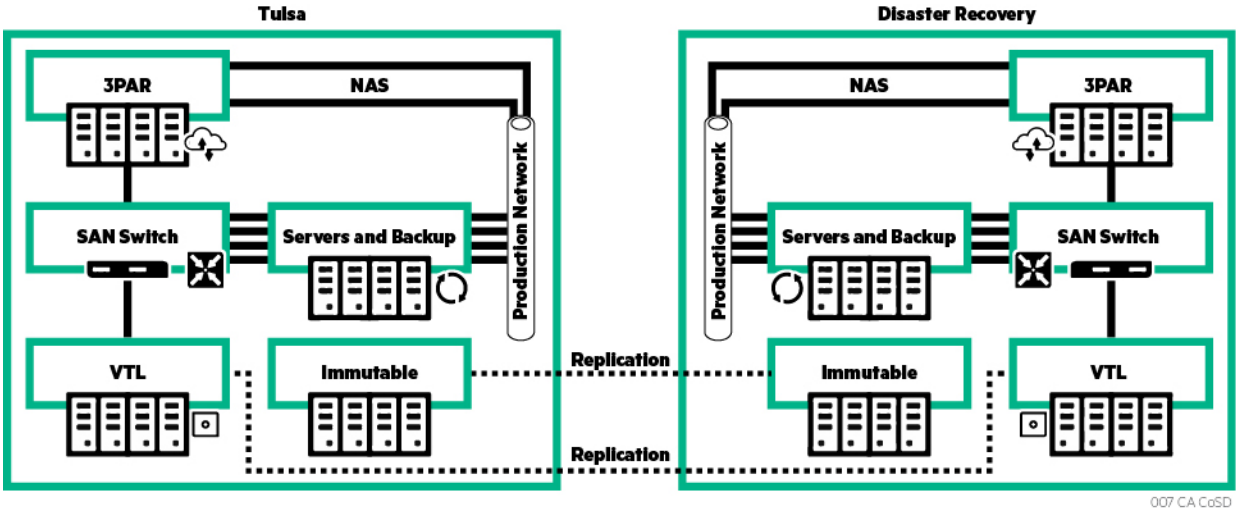
The existing production backup sets shall be copied to the new solution so that no backup set data is lost during transition. A StoreOnce VTL at the DR site shall join the backup environment as a replication target. Backups shall be replicated to the DR site. Full replication of backups shall serve two purposes:

- For applications that require a 72-hour or greater RTO for DR, these backups shall be used to restore service at the DR site.

For all applications, the duplicate backup system provides restore capabilities in the event the primary system is unavailable for an extended period of time. As services are migrated from Plano to Tulsa, Contractor's backup administration team shall create the service's schedule and policy in Tulsa and remove the service backup schedule and policy in Plano for those servers that have completed migration. These backup sets shall be replicated to the DR site as they are created. When all Plano services are successsfully migrated to Tulsa, the backup environment in Plano shall be decommissioned.

. Contractor’s solution shall incorporate 100% duplication of BUR data for the production data center at the DR site. The information shall be replicated between the sites using a dedicated network connection. The backup sets shall be stored in a Virtual Tape Library (VTL) at both locations. **Error! Reference source not found.**The figure below illustrates this solution.

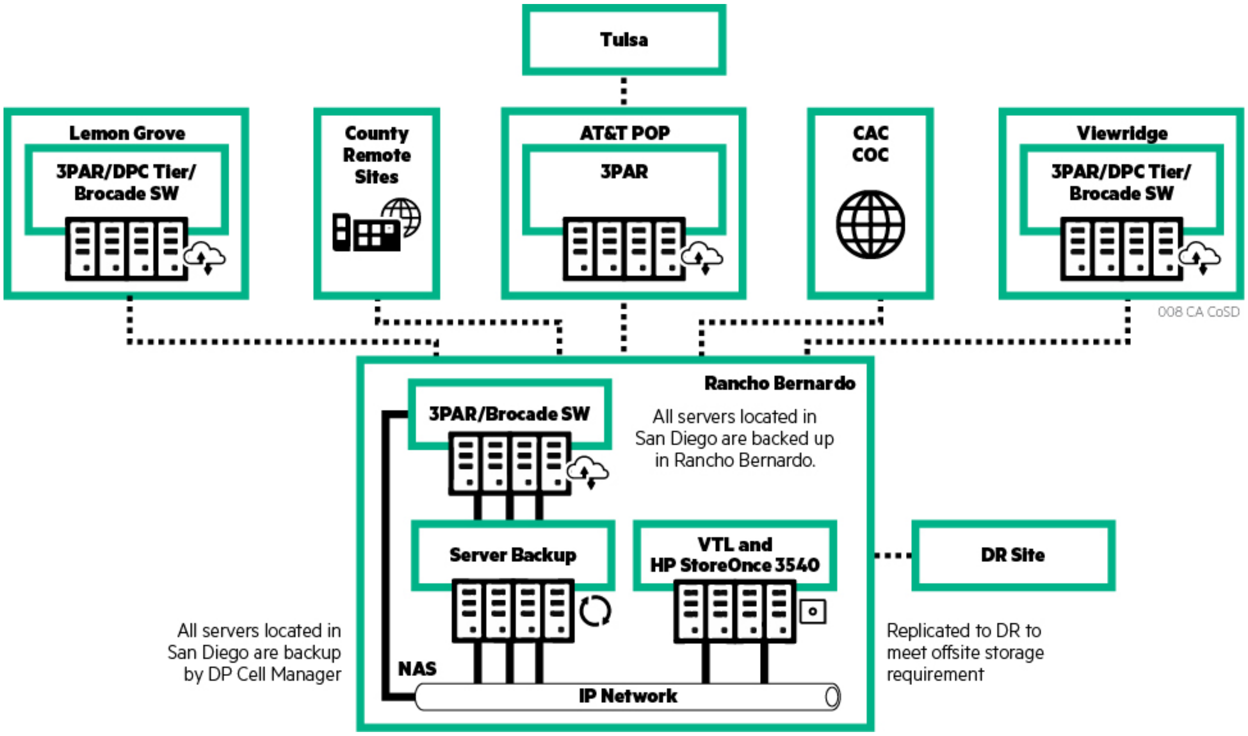
Future Logical View of Data Center Mid-range Server Storage / BUR



Contractor’s BUR solution shall provide 100% redundancy of backups in the Tulsa data center and the DR site, providing secure off-site storage of backup data, improved reliability, and quicker data recovery.

In the County’s document processing centers, Contractor shall create and consolidate backups at the Rancho Bernardo site using a small disk-based VTL, which shall be refreshed with a replacement of similar size. These backup sets shall also be replicated at the DR site in Colorado Springs. The figure below provides an overview of this solution.

Future Logical View of Document Processing Centers Storage / BUR


Tulsa
Lemon Grove
3PAR/DPC Tier/ Brocade SW
County Remote Sites
AT&T POP
3PAR
CAC COC
Viewridge
3PAR/DPC Tier/ Brocade SW
008 CA CoSD
Rancho Bernardo
3PAR/Brocade SW
All servers located in San Diego are backed up in Rancho Bernardo.
Server Backup
VTL and HP StoreOnce 3540
DR Site
All servers located in San Diego are backup by DP Cell Manager
Replicated to DR to meet offsite storage requirement
NAS
IP Network

Contractor's BUR solution for the data processing centers provides added reliability by backing up servers to Rancho Bernardo and replicating those backups for off-site storage at Colorado Springs.

Contractor shall perform backups of the AT&T POP, Lemon Grove, Viewridge and Rancho Bernardo (collectively known as the San Diego sites) in Rancho Bernardo. Contractor shall copy the existing Rancho Bernardo backup data sets to the replacement VTL to prevent backup dataset loss during the refresh. During the transition period, Contractor shall also replicate the Rancho Bernardo backups to the DR site for off-site retention. This approach provides several advantages:

- Elminates the need for a physical tape library and physical backup tapes, reducing the time required and complexity associated with performing backups.
- Eliminates the need to transport tapes for off-site storage by taking advantage of the DR site to perform this storage function.
- Speeds data restore activities by eliminating the time required to obtain backup tapes from a remote storage facility.

When the data center consolidation is complete, the production and Dev/Test, storage and BUR infrastructure, and O&M support shall be provided in Tulsa, with DR capabilities in Colorado Springs, Colorado. The Contractor backup administratiom team shall continue to provide centralized backup and recovery management from any location because all backup shall be to VTLs and replicated to the DR site over a dedicated replication network connection, eliminating any local tape handling requirements. All County data shall be backed up, as required.

Built on HPE Data Protector 9.0 software, Contractor's BUR solution shall provide comprehensive functionality designed for enterprise environments using a dynamic and agile data protection strategy. HPE Data Protector servers shall integrate with LDAP authentication services and support file inclusion and exclusion as an extra level of control. The Contractor administration team shall provide for auto-discovery of virtual servers, supports single-pass image backups of virtual servers, shall provide integration with HPE Data Protector with Oracle RMAN, and shall integrate with VSS to backup Shadow copies that have been created. It shall provide standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape, and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. It shall provide standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. HPE Data Protector shall provide real-time operational intelligence through a customizable BUR dashboard, that Contractor shall publish on the Service Portal.

Backups shall be weekly full backups and daily incremental backups. The backup retention period shall be customized within the policy that defines the backup, based on the type of data being backed up. Custom retention periods can be defined for specific Portfolio Applications, with County approval if the retention period requested is outside of the policy. Contractor shall categorize the types of data requiring backup and retention timeframes, as detailed inthe table below when developing the BUR solution.

Types of Data Requiring Backup and Retention Timeframes

TYPE OF DATA	RETENTION PERIOD
User unstructured Data (NAS): • H: Drives • S: Drives • Application Dev/Test • Application Production	90 days
Exchange 2010 (Email) • All Passive databases	14 days
Structured Data (Databases) • Dev/Test • Production	30 days
Application Servers • Dev/Test • Production	30 days
Infrastructure Servers • Domain controllers, SCCM Servers, Citrix, among others	30 days
Immutable Storage • Host based backups	30 days

For the County, the hardware solution shall be comprised of:

- HPE Data Protector Servers (7 cell managers and 9 media managers)
  - Cell managers are the servers that control, monitor, and store all backup object information
  - Media manager servers connect to backup target medion (disks, virtual tape or physical tape media) to access those media destinations.
- HPE StoreOnce B6600 disk-based backup media target, or VTL, in Tulsa. All Tulsa data center backups shall be replicated to a VTL in the DR site in Colorado Springs
- Contractor's StoreOnce 3540, at the Rancho Bernardo site, shall also be replicated to the DR site for off-site backup set protection.

Additional functionality provided by this solution includes the following:

- SharePoint – granular restore
- VM Server – snapshot restore

- Synchronized backup application for the Enterprise Document Processing Platform (EDPP).

  For cloud applications hosted outside of the Contractor data center, backup options shall be provided by the Cloud Service Provider.

Rationale: This approach shall provide improved reliability by eliminating a point of failure present if portions of data are backed up by different sites.

- Deployment plan for resources and use of facilities

Until the data center consolidation is complete, BUR services shall continue to be provided in the Plano and Tulsa data centers and the County document processing centers at Lemon Grove and Viewridge.

After the data center consolidation, Tulsa shall serve as the production data center and Colorado Springs shall be the DR site. The County document processing centers at Lemon Grove and Viewridge shall continue to serve the same functions. At this time, the space provided for the County in the Plano data center shall be released, and connectivity from the AT&T POP shall serve Tulsa only.

Contractor shall provide backup administrators in Tulsa with additional local staff to support the San Diego sites and shall be responsible for management of the immutable storage in Colorado Springs. They shall also manage the replicated images, 100% of which shall be replicated to the DR site.

SAN and SAN storage hardware shall be managed by Contractor USPS resources.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's BUR processes shall address the following types of backups:

- Virtual Servers – Snap Shot is VMware based for data within the VMware image, includes system state.
- Physical Servers – Host-based, using traditional backup agents that coordinate backup by looking at the files from the Host side.
- NAS – Fiber Channel, the backup system communicates directly to the array instead of the host to take the backup.

Specific process documents are discussed in the table below.

Process Documents

PROCESS	PURPOSE
HPE Data Protector Backup Verification Process	This purpose of this document is to verify that backup data can be restored and read. This shall be performed weekly by the BUR Administrator.
Preparing HPE Data Protector Cell Managers Prior to Scheduled Backups	The purpose of this document is to outline the steps preparing HPE Data Protector Cell Managers prior to scheduled backups. This shall be performed weekly by the BUR Administrator.
Upgrading the DPA Collector Agent on HPE Data Protector Cell Managers	The purpose of this document is to outline the steps to upgrade the DPA collector agent on the HPE Data Protector cell manager servers. This shall be performed weekly by the BUR Administrator.
Restarting Stalled or Unresponsive HPE Data Protector Backup Sessions (DOC ID BUR 0010)	The purpose of this document is to provide the process to be followed when In-progress backup sessions appear under Monitor in the HPE Data Protector Manager GUI, but attempts to view the

PROCESS	PURPOSE
	session result in the GUI freezing. This shall be performed as needed by the BUR Administrator.
StoreOnce Troubleshooting (DOC ID 0015)	Outline the process steps on how to troubleshoot the StoreOnce application. This shall be performed as needed by the BUR administrator
Workaround for Hung Sessions Due to Catalyst Media Server Timeout (DOC ID 0017)	Outline the steps and workaround procedures for hung sessions due to Catalyst media server timeouts. This shall be performed as needed by the BUR administrator.
How to Restart and Resume County of San Diego Backup Sessions (DOC ID 0018)	Outline the steps for restart and resume County backup sessions once failed objects and sessions have completely failed. This shall be performed as needed by the BUR administrator.
How to Kill the HPDP Session Using PID with Catalyst Devices (DOC ID 0019)	The purpose of this document is to outline the process steps on how kill the HPDP session using PID with Catalyst devices. This shall be performed as needed by the BUR administrator.
How to Archive Bit Reset Configuration for SQL Flat Files in HPE Data Protector (DOC ID: 0020)	Outline the process steps on how to archive bit reset configuration for SQL flat files in HPE Data Protector. This shall be performed weekly by the BUR administrator.
Resolving Latency on User and Data Shares (DOC ID: 0021)	Outline the steps and procedures for resolving latency on End-User and data shares. This shall be performed weekly by the BUR administrator.

Integration of data with Backup and Recovery Services, using required connectors such as Oracle RMAN and VSS.

Contractor shall support and maintain RMAN to write database backup files to spinning storage that is made available on the database server for the purpose of backups. The cost of the licenses for Oracle RMAN is not included in base services. The backup files on spinning disk shall then be captured in the next Contractor Data Protector backup. The files shall be stored on Contractor's tapeless backup media and replicated over a dedicated replication network connection to the DR site hundreds of miles away in Colorado Springs. Contractor shall support the creation of VSS (shadow copies), and the Contractor backup solution shall also be able to back up VSS shadow copies directly with a local copy of that backup written to the tapeless backup target and be replicated to Contractor's remote backup media.

6.14. Managed Print Services

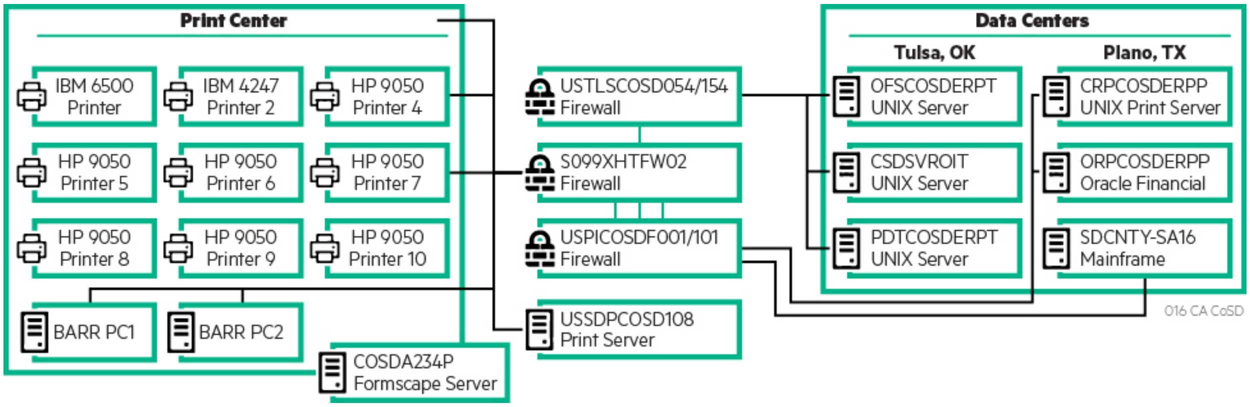
6.14.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide managed print services via the County print room facilities located at the Rancho Bernardo site. Contractor's print operations processing shall take place Sunday through Friday from 8:30 p.m. to 2:00 p.m. PT, with on-call support available as needed.

With the transition of the Juris-managed print requirements to Fujitsu, Contractor shall continue to provide managed print services of approximately 200,000 pages per month on average to meet Assessor and Tax Collector requirements. This shall be conducted at Contractor's print facilities at the Rancho Bernardo site. Contractor shall use the BARR print management tool to receive the files for printing. **Error! Reference source not found.**The figure below illustrates how print files are currently transmitted to Contractor's print center.

Transmission of Print Files to Required Printers



Migration from SA16 LPAR Mainframe to the Integrated Property Tax System (IPTS) shall consolidate and modernize the legacy property tax systems in a web-based system designed to vastly improve the efficiency of the property tax-collecting process. It shall also generate the tax bill files for printing. After implementation of IPTS, Contractor shall update processes and procedures associated with running daily print jobs for County Assessors and Tax Collectors.

Contractor shall provide the following services for the managed print framework component:

- Order supplies such as Contractor print toner and printer maintenance kits
- Ordering special forms and paper
- Provide support for microfiche

- Daily delivery of reports Deployment plan for resources and use of facilities

Contractor's primary print facility shall be the Contractor's Rancho Bernardo site and with the implementation of a disaster recovery solution, multiple geographically diverse sites shall have the capability to provide print services for the County. Print jobs shall be easily routed to any location. **Error! Reference source not found.**The table below summarizes the specific types of printing provided at each location.

Types Printing Provided at Each Location by Contractor

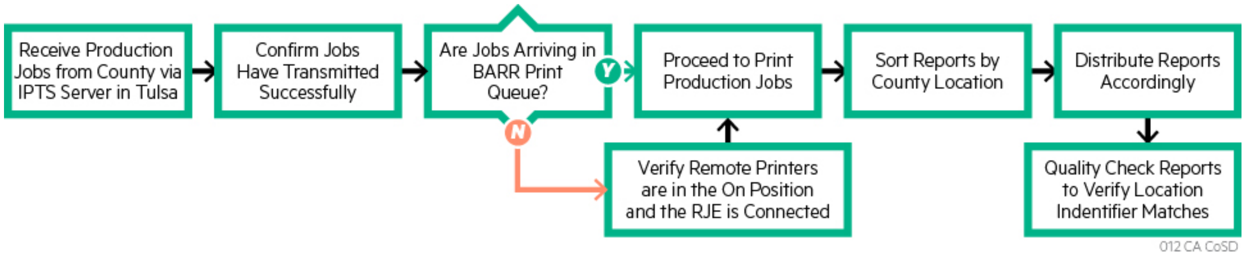
TYPE OF PRINTING	LOCATION
Laser and Impact Print	Rancho Bernardo
Annual tax bills, supplemental (small volume) tax bills, and tax bills that require manual intervention of the Treasurer-Tax Collector's (TTC) office.	Rancho Bernardo, with backup at Rancho Cordova
One-stop document and tax bill management—folding, envelope stuffing, and mailing	Rancho Cordova
Laser Print and Tax Bills (Dev/Test)	Troy, Michigan (trial) Rancho Bernardo Rancho Cordova

Contractor's dedicated staff shall work in the print center at the Rancho Bernardo site with responsibility for printing, distribution, and delivery of daily work.

- Key methodologies and processes in solution including year-to-year continuous improvement

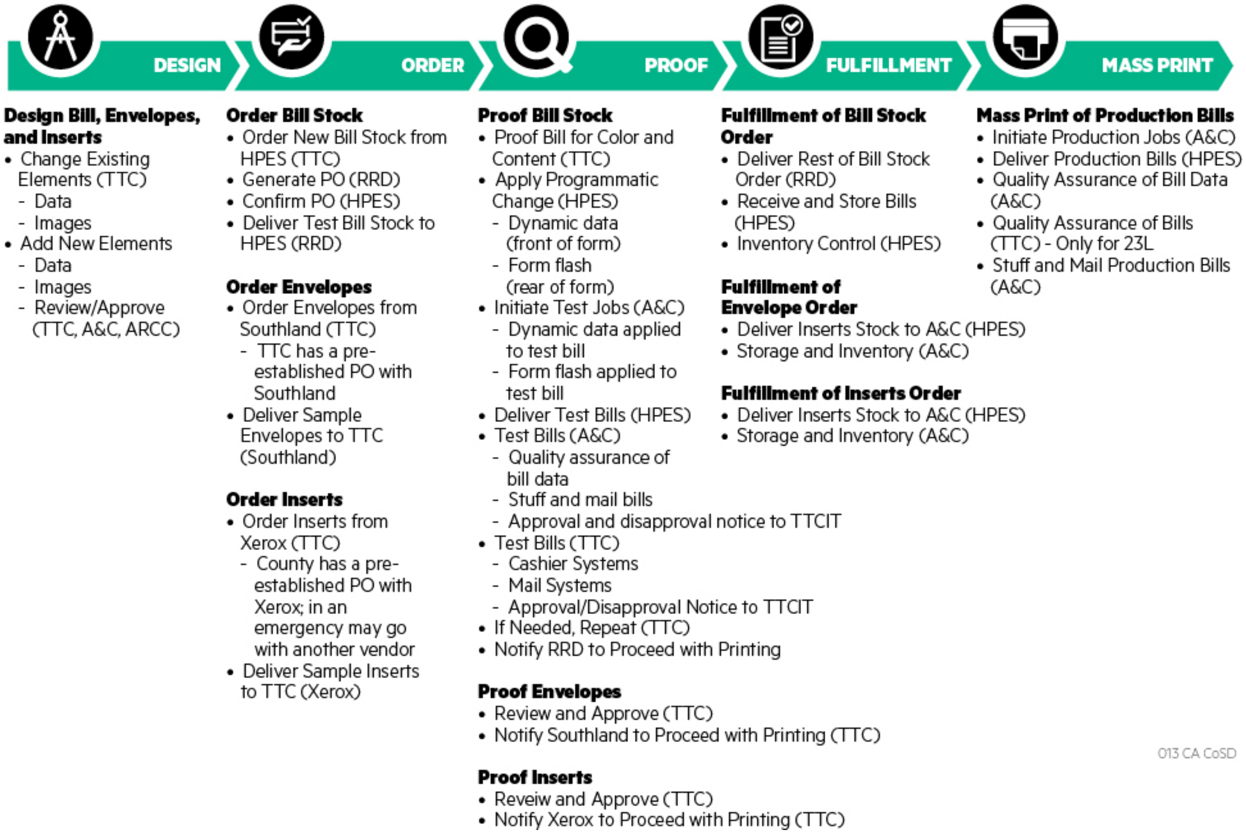
The figure below illustrates the process Contractor shall follow to receive print requests and print the reports for distribution to the County within the prescribed timeframe in Service Levels.

Contractor Process for Receiving and Printing Reports


Receive Production Jobs from County via IPTS Server in Tulsa
Confirm Jobs Have Transmitted Successfully
Are Jobs Arriving in BARR Print Queue?
Y
N
Proceed to Print Production Jobs
Sort Reports by County Location
Distribute Reports Accordingly
Verify Remote Printers are in the On Position and the RJE is Connected
Quality Check Reports to Verify Location Indentifier Matches
012 CA CoSD

Contractor shall follow the process checklist shown in the figure below and documented in the Standards and Procedures Manual.

Tax Bill Generation Process



Design Bill, Envelopes, and Inserts
- Change Existing Elements (TTC)
  - Data
  - Images
- Add New Elements
  - Data
  - Images
  - Review/Approve (TTC, A&C, ARCC)

Order Bill Stock
- Order New Bill Stock from HPES (TTC)
- Generate PO (RRD)
- Confirm PO (HPES)
- Deliver Test Bill Stock to HPES (RRD)

Order Envelopes
- Order Envelopes from Southland (TTC)
  - TTC has a pre-established PO with Southland
- Deliver Sample Envelopes to TTC (Southland)

Order Inserts
- Order Inserts from Xerox (TTC)
  - County has a pre-established PO with Xerox; in an emergency may go with another vendor
- Deliver Sample Inserts to TTC (Xerox)

Proof Bill Stock
- Proof Bill for Color and Content (TTC)
- Apply Programmatic Change (HPES)
  - Dynamic data (front of form)
  - Form flash (rear of form)
- Initiate Test Jobs (A&C)
  - Dynamic data applied to test bill
  - Form flash applied to test bill
- Deliver Test Bills (HPES)
- Test Bills (A&C)
  - Quality assurance of bill data
  - Stuff and mail bills
  - Approval and disapproval notice to TTCIT
- Test Bills (TTC)
  - Cashier Systems
  - Mail Systems
  - Approval/Disapproval Notice to TTCIT
- If Needed, Repeat (TTC)
- Notify RRD to Proceed with Printing

Proof Envelopes
- Review and Approve (TTC)
- Notify Southland to Proceed with Printing (TTC)

Proof Inserts
- Reveiw and Approve (TTC)
- Notify Xerox to Proceed with Printing (TTC)

Fulfillment of Bill Stock Order
- Deliver Rest of Bill Stock Order (RRD)
- Receive and Store Bills (HPES)
- Inventory Control (HPES)

Fulfillment of Envelope Order
- Deliver Inserts Stock to A&C (HPES)
- Storage and Inventory (A&C)

Fulfillment of Inserts Order
- Deliver Inserts Stock to A&C (HPES)
- Storage and Inventory (A&C)

Mass Print of Production Bills
- Initiate Production Jobs (A&C)
- Deliver Production Bills (HPES)
- Quality Assurance of Bill Data (A&C)
- Quality Assurance of Bills (TTC) - Only for 23L
- Stuff and Mail Production Bills (A&C)

Contractor shall use the BARR Systems Print Server to automate and control print and document output.

6.15. Public Key Infrastructure (PKI) Services

6.15.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall leverage the current MPKI 8.13 solution and use that as the foundation for additional PKI services. This solution shall be a fully extensible and redundant platform sized for the current project as well as future functionality. Key features and benefits of the Managed Symantec PKI solution shall be:

Key Features

- **Trusted, Cloud-Based Infrastructure:** Monitors, manages, and escalates across the globe with full DR and is certified as part of a SAS-70 security, WebTrust and specialized Government audits.
- **Broad Application Support:** Issuance of X.509 certificates that interoperate with operating systems, devices, VPN, mail, and web browser software. Certificate profiles for common applications are for email encryption and signing, and Adobe PDF signing.
- **Automated Certificate Life Cycle Management:** Automates configuration of authentication, encryption, and signing applications across platforms and browsers. Managed PKI service can automatically configure an End-User's browser, VPN client, mail client, or other application to use certificates. PKI Client also automates renewing certificates and prevents expired certificates from interrupting business continuity.

- **Enterprise Integration:** Integrate Managed PKI Service with a corporate directory to populate certificate meta-data, select and enforce certificate and application policies, and publish issued certificates. PKI Enterprise Gateway functions as a local registration authority integrating with hardware security modules to protect key material.

Key Benefits

- **Reduces PKI Cost and Complexity:** Managed PKI service's cloud-based approach dramatically lowers cost and complexity by eliminating the facilities, hardware, software, personnel, training, and maintenance expenses associated with deploying traditional in-house PKIs.
- **Simplifies the Administrator and End-User Experience:** Eliminates administrator tasks, and automates the process of provisioning certificates and configuring applications to use those certificates.
- **Maximizes Deployment Flexibility:** Not only can organizations deliver multiple certificate-based security applications from a unified platform, but they can also tailor the deployment to meet their needs.
- **Delivers Proven, Scalable, Reliable PKI:** Symantec’s procedures, policies, and infrastructure have been proven with large enterprises, governments, and manufacturers around the world

Self-service via the Service Portal shall be made available for specific use cases, for optional services or functions, such as certificates required for digital signing of expense reports.

The approved County solution for digital signing is the existing ARX/CoSign document. Contractor shall work with ARX/CoSign to develop and implement previously identified changes in the document signing solution to utilize the Symantec PKI certificates as part of transition.

Contractor shall integrate Symantec PKI with DocuSign CoSign. Currently the internal CoSign CA is used to generate and revoke certificates. This shall be replaced by a web service invocation to Symantec Cloud-based PKI. Today the enrollment process automatically occurs when a County End-User on a County machine attempts to sign a document or open any application that uses the CoSign client plugin (e.g., Word, Excel, Adobe Reader/Acrobat). This process shall remain unchanged. During the enrollment process, the CoSign appliances shall invoke a web service against the Symantec Cloud-based PKI to fulfill the certificate creation request. Once complete, the private key of the certificate shall be stored in the appliances’ internal store (as is done today). Subsequent requests to sign documents shall be fulfilled by the appliances only with no need to invoke Symantec services. This approach has already been successfully developed and deployed between CoSign and Comodo with production use by a number of customers. In addition to firmware changes, CoSign shall have to recertify their appliances if Federal Information Processing Standard (FIPS) compliance is required. Firewall rule changes at the County shall need to be created to allow connectivity between the appliances (currently in the data center zone) and Symantec PKI cloud. No changes are anticipated for Symantec. Additionally, no changes should be required for the CoSign clients residing on County desktops/laptops.

Contractor shall support the PKI solution using a combination of Contractor local resources and Contractor leveraged resources as part of the Identity Access Management solution. The PKI shall be supported per the Data Center support model as stated in Infrastructure Services. PKI functionality shall be supported by the local Security team and the Contractor Identity Access Management team, which shall support Active Directory and ADFS as well as other AD integrated solutions. Operational support functions shall include monitoring certificate status to identify when they are to be revoked or renewed as well as administrative management of certificate profiles and users.

- Deployment plan for resources and use of facilities

Contractor staff shall be located at the following sites to support the County:

- Rancho Bernardo. Primary location of dedicated Contractor staff specifically assigned to support the County. It includes centralized meeting space for engagements between the County and its contractors and Contractor personnel, including security staff and Contractor executives, and is the initial point of contact for the County. Test environments, training, and video conferencing are also housed at this site.

- Contractor Tulsa Data Center. This is the core data center that shall house the majority of the County IT infrastructure and delivery of core IT services as well as security services.

Certificate Practice Statements (CPS) state the terms and conditions associated with certificate use between County and external entities and typically come into play into the event of perceived misuse. The County needs to complete the CPS, and Contractor shall facilitate that process.

7. APPLICATIONS SERVICES

7.2. Application Maintenance and Operations Services

- Deployment plan for resources and use of facilities

Contractor shall utilize Contractor's Rancho Bernardo office, County locations as requested/required, and application development centers in El Paso, TX and Pontiac, MI.

7.2.1.1. Process and Procedures

Applications Maintenance & Operations (M&O) Services

Contractor shall provide a bundled approach. Applications shall be bundled based on level of service appropriate to each bundle. On a quarterly basis, or as requested by the County, Contractor shall review the application portfolio with the County to determine growth or reduction of applications and determine if a bundle adjustment is required. As a part of the review, Contractor and County shall establish an Application Review Board (ARB) to evaluate the activity and provide "move forward" recommendations. The ARB shall consist of County representatives and Contractor representatives, as further detailed in the Standards and Procedures Manual. The Application Review Board, with participants determined by County CIO and Contractor AE, shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications M&O FFP bundles or the FFP Dev/Test RU. Annual pricing reductions to the FFP M&O shall be 2% beginning Contract Year 2.

The applications are separated by bundles types into three groups—(full support, coordinated support, and Software as a Service (SaaS) support) across the five business areas.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.
By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be a better grouping as some departments often uses a single low-org regardless of department or division.

Applications M&O Services shall include all services (e.g., labor), software, hardware, and required system environments. For example, Contractor is responsible to provide Break/Fix environments to support an application (e.g., to test new patches or versions), that is included in the FFP Apps M&O RU, and FFP Dev/Test RU.

High Level Key Benefits to the FFP Apps M&O

- Predictability of costs
    - One monthly charge (by County, Group or Low-org)
    - Discount offered by Group or by County options
- Predictability of budgeting
- Cost reduction Year-Over-Year beginning CY3
- All PA-IDs are covered
- Maintenance of applications are more timely
    - Not reliant on additional department funding for standard/routine application patches and updates (including 3rd party)
- No limit to skillset utilized to resolve issues
    - Eliminating the dispute when a break-fix incident requires an architect or engineer yet the NDSR does not support that skill
- Contractor assumes the risk of increasing costs

The priority levels assigned to all Portfolio Applications as of the Contract Effective Date (CED) shall remain the same for the Term of the Agreement unless otherwise agreed upon by the parties in accordance with the Agreement.

- Solution to meet the requirements

Contractor's solution shall include the transition of all of the County's Applications M&O (M&O) activities to the FFP model. In Contractor's discussion below of 10 high-level M&O requirements that follow, Contractor shall distinguish between Applications M&O activities and Application development activities.

Contractor shall develop process improvements automation to reduce the cost of M&O services over time. All application patches for routine maintenance and/or restoration of services shall include UAT.

Contractor has assembled the County applications into 3 options/bundles where each option may have 3 support models full support, coordinated support and cloud-based Software as a Service (SaaS) support.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.

By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be better grouping as some departments often uses a single low-or regardless of department or division.

Full support comprises a full range of application activities from Break-Fix incidents response, restoration of service, M&O activities such as installation of patch/upgrades for routine maintenance activities. Full support includes those applications where Contractor has the access and ability to affect change either with or without the participation of a third-party vendor.

Coordinated support applies to applications where Contractor hosts the application but does not have security access or the ability to affect change. Contractor shall engage with the vendor and coordinate the necessary change(s). When possible**,** provided by 3rd party and approved by the County, M&O activities such as coordination of Break-Fix incidents response, restoration of service, installation of patch/upgrades for routine maintenance activities shall be performed.

SaaS Support are cloud-based applications where Contractor does not host the application and has no ability to affect a change. Contractor shall contact the SaaS provider and keep the County informed of the status of the issue or change.

On a quarterly basis, the ARB shall review the Applications Portfolio to evaluate the number of applications that have been added or retired and determine whether the RU warrants adjustment. This review shall also occur upon County request or in the event Contractor identifies a material change, as that term is defined below.

Material changes are additions or deletions of Portfolio Applications that affect the M&O support or server environment and that meet any of the following criteria:

1. Fifty (50) or more End-Users
2. Adding or deleting five (5) or more servers to Dev/Test
3. Adding or removing an app representing >30% of a billing low-org

As needed upon recommendation of the ARB, the County CIO and Contractor AE shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications FFP bundles or the FFP Dev/Test RU.

Unless modified by a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or upon the expiration of a stated warranty period, whichever is later.

For addition of a large application (e.g. ConnectWellSD) or a complex enhancement to an existing application (e.g. adding Open Enrollment to PeopleSoft), which requires 1500 hours or more of labor, the County shall deliver a Service Request to Contractor to perform M&O activities for up to six (6) months as time and materials. During this time, Contractor shall provide a report of M&O support, “actuals,” and a detailed report of hours and tasks performed to determine the future adjustment to the appropriate FFP bundle. The ARB shall review the report of the six (6) month sampling for reasonableness and shall then provide a recommendation to the County CIO and Contractor AE.

Restore Service Levels

First, Contractor shall validate the restoration requirements for each application and structure Contractor's team to meet those requirements. If an application requires 24x7 onsite support for restoration of services, Contractor shall staff and schedule the response team to be sure M&O staff is available 24x7. If an application requires 24x7 on-call support, Contractor shall schedule staff to be standing by to respond to an outage 24x7. Applications that require less than 24x7 shall be supported in accordance with priority to specific County business needs. Contractor shall provide a Monday through Friday, 6:00 a.m. – 6:00 p.m. support window for all other applications;

Contractor shall build and enhance applications to prevent outages. As part of application portfolio maintenance, Contractor shall design and develop applications to be hardened and not fail. Contractor shall evaluate the supporting software middleware, and hardware for the application to verify the application's supporting components deliver required Service Levels without disruption. Contractor's team shall thoroughly test the application's new functionality, regression test unchanged functionality, and performance test the application executing simulations in a Dev/Test environment before implementing a change.

Contractor shall operate to restore applications functions as quickly as possible in the case of outage, whether application or infrastructure based. Contractor shall follow the Incident Management process detailed in, Cross Functional Services. Technical support shall triage as soon as they are notified by the Service Desk, and work the issue until functionality is restored. For mission-critical outages, the support staff shall use additional SMEs as needed and reach back to vendors and suppliers when necessary to resolve the outage. The Service Desk, with information from the technical support staff, shall notify Contractor management of the outage, and Contractor management shall notify County management.

When a change to the application is required to resolve the outage, Contractor shall perform the necessary application changes, data updates, and/or third-party software patching, to restore services in accordance with County emergency fix process. All application patches for routine maintenance and/or restoration of services shall include End-User acceptance testing, as desired by the County.

Contractor's application services team shall build new applications and enhance existing ones to prevent outages. Contractor shall make recommendations for changes to applications, and perform monthly analysis to identify defect rates, annual cost, and technical obsolescence within applications. As part of the ARB, Contractor staff shall work closely with the County board representatives and present outage incidents, provide recommendations regarding technical obsolescence, and review portfolio additions and deletions. A standard agenda shall be developed and reviewed at each meeting.

Production portfolio applications maintenance

Contractor's plan to maintain the portfolio focuses on keeping production up and running with a goal of no disruption to the County. In addition, Contractor shall continually improve applications to optimize performance and apply patches from third-parties.

Contractor shall make maintenance changes to production applications upon a County-approved request for change (RFC). Contractor shall meet weekly with the County to review the pool of RFCs and determine the priority and whether it can be approved for implementation. Contractor shall schedule the implementation of approved RFCs based on County priorities and approval.

When Contractor implements an RFC to fix a bug, install a patch, or implement an upgrade as part of M&O, Contractor shall follow Contractor's existing SDLC methodologies and the County's change and release management processes. Contractor shall functionally test RFC implementations and perform regression and performance tests. While implementing the change, Contractor shall build in warnings, notifications, and processes to provide application support of the RFC during operations if needed.

In conjunction with the County, Contractor shall define the authorization requirements (security) for End-Users, roles, and schemas and shall provide provisioning and de-provisioning of End-User and service accounts for the portfolio applications as authorized.

If a firewall change is required by M&O activity, it is covered under Apps M&O. If the firewall change is required by a new application or new End-User request (adding DA or hospital access), it shall be costed as part of the project.

With every service restoration fix, patch, or minor maintenance implementation, Contractor shall update the appropriate portfolio application documentation in accordance with the new functionality in production and all application document artifacts impacted by the RFC, including application document libraries, configuration management databases, and application management system, known as AppsManager.

Contractor shall evaluate the applications architecture, configuration, and system upgrades and identify opportunities for improvement. When opportunities are identified, Contractor’s team shall initiate new RFCs and implement them after approval by the County.

In addition to implementing changes, Contractor’s team shall support the application in production. Contractor shall build an application support team with the right number of staff with the right skills set and expertise to support the applications in production. RFCs are implemented in adherence to Contractor’s SDLC process, the County’s change management and release management procedures, and County governance approvals. Contractor shall provide services based on ITIL-aligned processes, CMMI standards, and other leading practices as appropriate. Contractor’s project managers and applications subject matter experts (SMEs) shall work with the County and its delivery and application product owners to build a project plan to provide predictable, repeatable, and successful results.

Contractor’s M&O services team shall provide planning, monitoring, and schedules for new applications as they are placed into production. The team shall respond to warnings and notifications generated by the applications and fix the issue that triggered the warning or notification. Contractor’s infrastructure support team shall monitor the operating environment supporting the applications. Contractor shall triage application and hardware incidents and take the appropriate action to restore service.

Contractor shall execute End-User administration for the applications following the application’s processes and procedures for End-User administration, including the necessary County approvals. Contractor shall update the appropriate portfolio application specific documentation as necessary, as well as Service Desk scripts, application data elements in AppsManager, and the Service Portal.

Contractor shall perform periodic reviews that may result in recommendations for application security improvements, product and software changes, or improved performance and cost savings. Contractor shall provide recommendations to County business owners and CTO to make sure the performance of the applications portfolio is optimal.

As part of M&O activities, Contractor’s staff shall perform special testing for events such as public holidays, end of financial year, end of calendar year, and daylight savings time.

Application M&O Scope

M&O activities shall include executing the process to maintain application interfaces and coordinating with third parties to manage those interfaces. M&O includes performing the necessary preventive maintenance, routine system patching, application upgrades and code releases, but only as required for restoration of services, mitigation of security vulnerabilities, and implementation of a maintenance release. Notwithstanding the foregoing, if a routine system patch, restoration of service patch, or application upgrade includes an Enhancement, as that term is defined below, the implementation of which exceeds reasonable Contractor work effort, Contractor shall have the option to escalate the review of cost allocation to the ARB.

An Enhancement is defined as any product change or upgrade that increases software or capabilities beyond original specifications. It can also be distinguished as an improvement (enhancement) of an existing application capability or a totally new capability.

Applications M&O shall not include County requested Enhancements (including security Enhancements) or County requested application upgrades (e.g. PeopleSoft 9.2 upgrade or SharePoint 2013 upgrade).

In the event of a service outage resulting from application or infrastructure abnormalities, Contractor's M&O staff shall perform necessary code fixes to restore service in accordance with the bundled service. The SDM shall drive incident management activities and provide ongoing communication to the client. As a result of the service restoration, Contractor shall execute the necessary root cause analysis (RCA) to investigate the outage issue, following the RCA process as described in Cross Functional Services. These activities shall include analysis, design, coding, testing, data conversion, documentation, End-User coordination and communication, and production turnover activities and the management of these activities for restoration of service. Based on the RCA findings, Contractor shall recommend modifications to the application to prevent future outages, including those attributable to a Third Party.

Align Maintenance Activities with County architecture standards, guiding principles, and architecture bricks and patterns

All Architecture activities required by Apps M&O shall be included in the Applications M&O RU. Contractor's shall align with County IT architecture standards while participating in the process to improve, refine and enhance them. Contractor shall monitor technology trends, best practices, and products within the IT industry, recommend enhancing County processes when appropriate, and Contractor shall provide a repository to document and manage standards, available through the Service Portal. Contractor shall build any additions into standard processes and practices.

On an agreed to schedule, Contractor shall participate in annual technical and business planning sessions, including bricks, to enhance standards, architecture, and project initiatives.

Contractor shall perform maintenance activities following the Standards and Procedures Manual as updates occur and shall implement all modifications to make sure Contractor's staff is aware and trained.

Provide M&O services for portfolio applications in production environments including servicing middleware and other application supporting components.

Contractor shall maintain both nonproduction and production environments for applications. This maintenance shall include keeping non-production configurations synchronized with production. Contractor's M&O staff shall keep the application and its supporting components, such as middleware, synchronized. Contractor shall accomplish this by updating supporting components using the same processes Contractor uses to update the applications. Contractor's M&O staff shall initiate an RFC to update components and implement the update when approved and scheduled by the County.

Contractor shall put steps in every project schedule to update the non-production environments with any approved component upgrade.

Maintain accurate and continuous prompt updates to asset and system documentation

Each approved Request for Change (RFC) shall include a step to update application documentation. This shall include updating asset and system documentation and tools. M&O staff shall be responsible for the technical accuracy and specific details of the update, and staff leads shall review the changes for accuracy and completeness.

Validate cross-framework integration and communication is conducted for application incidents, outages, maintenance work, planning purposes and all changes

Contractor shall validate cross-framework integration by regression testing application bug fixes and enhancements prior to production implementation. Contractor shall build and maintain test (Break/Fix) environments that include or simulate cross-framework integration, and Contractor shall build Contractor's test plans to include cases to test the frameworks.

Contractor shall keep County stakeholders informed on the full range of application activities from incidents, M&O activities, and changes.

The applications team shall follow the outage management communication process.

Provide services in alignment with ITIL and CMMI standards to ensure predictable, repeatable, and successful results

Contractor shall use industry best practices to enhance effective planning, execution, tracking, and delivery of services to the County. Contractor's repository shall provide the backbone of Contractor's process improvements and includes templates, guidelines, checklists, and lessons learned. It complies with recognized industry standards, including the Project Management Institute's (PMI) Guide to the PMBOK, ITIL, International Organization for Standardization (ISO) standards, and the practices incorporated in CMMI Institute's Capability Maturity Model Integration (CMMI).

Implement new patches and versions (within the current release), prioritizing patches that address security vulnerabilities

Contractor shall implement new patches and versions under M&O following the existing RFC process. Contractor shall create a plan to communicate, test, and implement each patch or version. All patches and versions shall be discussed with the County business owner and CTO to determine criticality, scope of change, priority, and timing. Following successful testing, Contractor shall submit an RFC for approval and scheduling.

When competing patches are released, patches that address security vulnerabilities shall get priority, along with those that fix critical issues. Next priority shall be patches that address minor issues, those which have a workaround available, and lastly patches that address issues that have not impacted County users.

Perform Maintenance Services that include Preventive, Adaptive, and Perfective Maintenance

Contractor shall perform application maintenance as part of M&O service. Contractor understands the objectives of preventive, adaptive, and perfective maintenance with respect to M&O to be as follows:

- **Preventive Maintenance** – Maintain application reliability to prevent issues from emerging in the future
- **Adaptive Maintenance** – Modify the system to adapt to changes in the business environment.
- **Perfective Maintenance** – Modifications and updates to sustain application usability and improve its reliability and performance.

Contractor shall perform preventive maintenance to resolve known problems and defects; perfective maintenance to optimize and tune performance; and adaptive maintenance to remediate impacts resulting from interfacing application changes, changes to application middleware, or changes to the infrastructure.

- Processes in solution including year-to-year continual improvement.

Contractor shall use County-approved procedures and standardized industry processes and governance based on PMBOK, ITIL, and CMMI as well as the Contractor operations excellence support methodology and repository of best practices and lessons learned. By driving the adoption of standards, taking full advantage of developments in technology, and being flexible and agile, Contractor shall help the County transform and manage its environment to achieve a balance of maintenance and innovation, reliability, and change. These methodologies shall enable Contractor's team to prevent outages and defects before they occur by thorough testing during the development phase. In the event of an incident, however, Contractor's methodology provides responsive M&O for fast and effective resolution.

For continual improvement, Contractor shall regularly review incident reports, RCAs, and application performance data so that applications are optimized appropriately. Contractor shall also monitor industry best practices as well as emerging trends and new technologies to determine if a different solution provides a better outcome. All this information shall be shared and reviewed with the CTO.

Contractor shall develop process improvements and automation to reduce the cost of the M&O services.

Process used to migrate developed Applications into (and retire/decommission Applications from) the Applications Portfolio, including the approach, data requirements, timeframes, and analytic approaches to ensure a reasonable fixed price for Applications M&O Services.

Throughout the year, applications are added and retired from the Applications Portfolio. The County initiates additions and retirements as an approved request.

When adding an application to the M&O portfolio, unless otherwise requested by the County through a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or the expiration of a stated warranty period, whichever is later.

Addition includes updated Service Desk scripts and entry of application details into the AppsManager tool. Support for the application shall be part of the FFP M&O.

For addition of a large, complex such as Connect Well San Diego or implementation of an additional module to an existing app, a service request shall be delivered to Contractor to perform M&O activities for up to 6 months.

Large, Complex is defined as a Portfolio Application modification estimated at 1500 or more total labor hours.

During this time Contractor shall gather and report M&O support 'actuals' to determine the future adjustment to the appropriate FFP Bundle.

Conversely, if an application is to be removed (retired) from the M&O portfolio, the M&O team shall perform all functions required to retire that application, including decommissioning the infrastructure and updating Service Desk scripts. Applications shall be retired by the direction of the County using a non-billable Service Request.

Contractor shall develop process improvements and automation to reduce the cost of the M&O services.

Third-Party Software packages are updated to current versions. Frequency with which Contractor's organization typically implements upgrades. The process Contractor undertakes from initial testing through production implementation and the value added by this process. Describe the process which shall be followed to keep County representatives aware of the availability of Third-Party Software package upgrades.

Approach. Contractor shall catalog and track all third-party software used by the County to make certain that software is maintained to the current versions. Contractor shall report to the County application primary contact on third-party software with upcoming updates. Contractor shall meet with the County and shall recommend third-party software upgrades. All changes shall follow Change Control Review Board (CCRB) in accordance with County processes and procedures for third-party software.

Frequency. Contractor shall proactively track upcoming updates to third-party software through the Internet, direct contact of third parties, and/or by announced vendor notices or technical updates. Upgrade frequency to third-party software shall depend on the software vendor and County direction.

When patches or upgrades are published for release, Contractor shall notify the County application primary contact that a release exists. Upon approval of the County CCRB, Contractor shall initiate the process for upgrading third-party software as outlined below.

Contractor shall conduct weekly meetings between Contractor and the County CCRB in which decisions on upgrades are addressed. If greater frequency is required, Contractor may request on a case-by-case basis an emergency meeting of the County CCRB specific to any urgent upgrades that Contractor believes require immediate County attention and approval (for example, patches that remediate security vulnerabilities).

Process — Testing Through Implementation. Once Contractor receives an upgrade, Contractor shall stage that upgrade and run tests in accordance with Contractor's Standard Procedures.

Initial testing shall start with the development of a testing plan and installation of the patch release/upgrade in a testing environment. Staff from Contractor and the County shall test the new version of the third-party software.

User acceptance testing (UAT) may include specific testing scripts and scenarios, depending on the application and the amount of enhancement. Once UAT is completed, results shall be presented to the County for approval and signoff.

Upon UAT approval, Contractor shall schedule and prepare for software installation into the production environment. This process shall be consistent with existing County processes and lends itself to a predictable, reliable, and controlled approach for upgrading third-party software for the County.

Upgrade Availability Communication. Contractor shall meet weekly with the CCRB to review the recommended changes. Each proposed change shall be approved by the County CCRB and the County representative. At such time that the proposed change is approved, Contractor shall schedule the change to accommodate the application downtime window.

Applications Services Framework

- Use of Tools

Contractor shall provide automation tools such as Contractor's APM which provides a 360-degree view that verifies the performance of desktop, web, and mobile apps for on premise, cloud, or hybrid environments, as well as Cascade, SCCM, and various other network related tools

- The implementation of APM shall enhance Contractor's ability to:
- Provide end-to-end visibility of transactions including back-end systems and mainframes
- Monitor the End-User application experience and services
- Quickly find and resolve application performance issues
- Collaborate with application development teams to effectively resolve application and transaction issues
- Reduce mean time to repair critical business transactions
- Monitor performance of applications deployed to a cloud or virtual environment
- View application performance alerts anytime, anywhere on the End-User's mobile device.

Contractor shall provide and use Cascade, SCCM, HPE Operations Manager, and other network and system related tools and reports to identify and correct issues in the environment related to applications, desktops, web, mobile applications, and others. The addition of APM shall assist to close the circle of the end-to-end reporting so that Contractor can be proactive in addressing systemic issues and making sure Contractor's solutions are running as expected to support the applications.

The SDMs shall work with the application SMEs, vendors, and the Enterprise Problem Manager to make sure that any and all items identified through these tools and reports are being acted on quickly to reduce the amount of impact to the End-Users as described in Service Delivery Management and Problem Management Services.

Contractor shall provide Project and Portfolio Management (HPE PPM) module for consolidating, prioritizing, and fulfilling application services activities and development projects so the County has visibility into all of the demands on the infrastructure. Its web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels are updated automatically as each request is processed.

Contractor shall provide a Service Portal that shall automate Service Desk ticketing, for incident and break/fix resolution.

On an ongoing basis, Contractor shall evaluate additional tools to further automate M&O activities, such as self-healing tools and discuss any recommendations with the County.

- Alternate Time & Materials model to provide Applications Maintenance and Operations services

Time and Materials (T&M) or Non-Discretionary Service Requests NDSR-like ("NDSR") Process

NDSR Rules of Engagement:

- All applications shall have an NDSR
- NDSRs shall be by PAID, Low-org, Department or Group
- Funding amounts shall be established for the County fiscal year
  - Invoicing shall be monthly based on actuals
  - If utilization reaches 80%, Contractor shall notify the County
  - If utilization reaches 90%, Contractor shall submit a Change Request to increase funding*
    - Regardless of available funding, all T&M activities shall be billed to the Low-Org associated with the corresponding NDSR (in the event the change request is not approved in time to cover a break-fix activity)

- Contractor shall provide estimates (based on actuals) to assist in establishing appropriate NDSR funds on a monthly basis to forecast trending

- NDSRs cannot limit the job classification approved to work on a break-fix
  - Charges to the County are task-based, not person-based

Note: If a NDSR requires chronic changes (meaning the County user set the funding intentionally low, thereby requiring change requests on a regular basis to replenish the funding), Contractor shall notify the County CIO for resolution.

7.2.4. Application Programming

7.2.4.1. Process and Procedures

Application Programming

Application programming are those activities associated with the programming, scripting, and configuring of application modules to support M&O activities.

Contractor shall perform applications programming using and adhering to the County's technical and architectural standards as well as standards and procedures, performing all necessary steps to complete M&O tasks. Contractor shall use Microsoft Team Foundation Server (TFS) to create working directories and store source code.

7.2.5. Application Integration and Testing

7.2.5.1. Process and Procedures

Application integration and testing shall be services that confirm the individual application framework components work together properly and, as a whole, perform its specified functions.

Contractor shall plan and develop Contractor's testing procedures to meet County requirements and policies. Contractor shall document the testing procedures in the Standards and Procedures Manual, including procedures to be followed by an independent testing team as needed. Contractor shall develop an overall test plan for M&O releases that includes the test strategy, coverage, scenarios, test bed, test data, methods, schedule, and responsibilities.

Contractor shall build and maintain an application testing environment that has been refreshed with production data. If necessary, Contractor shall build data masking programs to disguise production data. Contractor shall build test cases to test the new functionality or components based on the requirements and determine which valid data is required to appropriately test the application as well as the various testing phases. Contractor shall create a set of test cases to test the application end-to-end, new and existing functionality, application security and application supporting components, and infrastructure, when needed, to support M&O activities. Benchmark test cases shall also be created and run to properly execute regression testing. Contractor shall provide a reference to link requirements and test cases.

Contractor shall execute the test cases while following the standard testing procedures and verify that the results meet County testing requirements. Contractor shall track defects in a County-approved tracking tool and shall correct retests functionality to validate repairs. In addition to testing the application, Contractor shall provide an UAT environment, if needed, it shall include the necessary data. Contractor shall provide support to the County in its UAT testing effort and provides access to the defect tool for entering found defects. Contractor shall assess and report potential risks to production of implementing a change and only implement after County approval.

Contractor shall manage the various testing environments including the application data, application releases, and supporting software and components. Contractor shall stage the applications changes in the appropriate system in preparation for production implementation. Contractor shall provide support to these implementations, track their migration status, and verify the implementation of changes into production. Contractor shall define the test-to-production turnover requirements and instructions for each project or release and report the results, which shall be shared with the County.

7.2.6. Application Implementation and Data Migration

7.2.6.1. Process and Procedures

Application integration and testing for M&O activities shall be defined as those activities associated with the installation and migration of new patches and maintenance upgraded components to the production environment.

Contractor shall create a detailed plan for each M&O release. Contractor shall have a "go/no-go" checklist, after approval of UAT. All M&O releases shall include rollback steps and, Contractor shall update any affected application documentation and production application support documents and procedures as needed.

Contractor shall execute, coordinate, and communicate with the County for all releases and associated activities. For each patch and/or upgrade, Contractor shall perform the needed steps of the SDLC such as requirements analysis, design, development, and testing as appropriate for M&O activities. Contractor's deployments shall follow the County's change and release management processes and are compliant with client change management policies. Documentation shall be regularly updated, including the Standards and Procedures Manual and Service Desk scripts. Contractor shall execute the deployment in production once approved by the County and Contractor shall synchronize the production and non-production environments.

7.2.7. Application Documentation

7.2.7.1. Process and Procedures

Application documentation is defined as the development and maintenance of documentation for all applications. Contractor shall continually improve application documentations, providing new and updated documentation when required for system specifications, technical documentation, operational processing flows, system installation, application production support manuals, configuration plans, tuning instructions, release notes, and solution design as needed for M&O upgrades and patches. Contractor shall execute application updates as needed with every release, including patch and update releases as defined in "Production portfolio applications maintenance".

Contractor shall build and maintain documentation folders for each application, which shall be stored online with County controlled End-User access. All documentation created or updated for a release shall be stored in the folder in DocVault and shall be updated at the same time as the release implementation.

This shall help to keep the documentation in sync. Contractor shall store updated code and application components in the code CMDB to maintain the application currency and versioning.

Contractor shall also assist the County with developing, maintaining, and enhancing its application DR process and related documentation.

7.2.8. Application Training

7.2.8.1. Process and Procedures

Application training is defined as the implementation of training programs for contractor personnel to help preserve and enhance their knowledge and understanding of applications.

Contractor shall develop training for new and existing staff on the applications as necessary for M&O activities. When Contractor builds a patch or service restoration release, Contractor shall update the application training plan as needed.

During application operations, Contractor shall provide technical training and knowledge transfer to existing County support personnel, as well as materials related to the technical aspects of applications, as necessary. Contractor shall develop, document, and maintain the Policies and Procedures Manual, training, and knowledge transfer procedures that meet the County's requirements and policies.

In addition to training users, Contractor shall conduct new and refresher training programs for Contractor's personnel to preserve and enhance the knowledge and understanding of the applications and the underlying technologies and frameworks on which they are built. The training shall include industry standard certification as well as external training on the latest releases of databases, middleware, enterprise platforms, and applications as required.

Contractor shall train Contractor's development and M&O staff to support application development and changes when implemented into production. Contractor shall follow ITIL-aligned processes for training documentation. Additionally, Contractor shall develop and conduct cross-training to facilitate smooth transitions between Contractor personnel as required and to make sure backup personnel are in place for each application.

Delivery of End User training, including the location and method of training, frequency of training, and documentation provided with training.

End-User training shall include online training or videos to specialized in-person classes or seminars.

Contractor shall develop online training appropriate to the projects. This may include Adobe Captivate vignettes, videos, or posted documentation and frequently asked questions (FAQs).

For specialized in-person training, the County currently uses the 200-square-foot Contractor/County training center in Contractor's Rancho Bernardo location. Contractor shall continue to maintain and make that space available to the County. The center provides 36 County-imaged desktops hosted on the County of San Diego Network and provides a quiet, controlled environment. The center's simulation environment shall accommodate User Acceptance Testing (UAT) if requested, which allows the County to test features and functionality prior to deployment.

The facility shall provide printing and projection capabilities to support a successful training experience. This facility shall continue to be available as well for County trainers to train County staff.

Major releases may require online and classroom training for the End-User community on a scheduled basis, while minor changes may require only an update to procedures or processes and notification to the End-User to use the new process.

7.2.9. Application Quality Assurance Services

7.2.9.1. Process and Procedures

Application QA services is defined as a systematic, planned set of actions necessary for software update/development processes to conform to established functional technical requirements. It also includes the managerial requirements of keeping the schedule and resources within budgetary confines.

Contractor shall create, update, and maintain a QA management approach for applications updates. This shall include the following QA components:

- Quality management approach
- Effective software engineering technology
- Formal technical reviews applied during the SDLC process
- Multi-tiered application integration and testing strategy and implementation
- Control of software documentation and associate changes
- Procedure to measure compliance with software development standards
- Measurement of QA metrics and reporting mechanisms.

Contractor shall submit Contractor's QA management approach to the County for approval, after which it shall be added and kept current in the Standard and Procedures Manual.

Contractor shall determine QA metrics for each release and reports these to the County. Contractor shall communicate configuration management items, tracking them to Contractor's Systems of Record that accurately depicts the environment. These shall be updated to reflect all new changes, which shall be made with a change record processed through HPE Service Manager that keeps Contractor's information accurate.

7.2.10. Database Administration

7.2.10.1. Process and Procedures

Database administration (DBA) shall be defined as activities associated with the maintenance and support of databases.

Contractor shall define DBA requirements and policies for the application databases, including authorization requirements for end-users, roles, and schemas. Contractor shall develop a Standards and Procedures Manual database administration procedure that meets the County's standards and policies. Contractor shall develop and provide database roadmaps for planning and portfolio management.

Contractor's DBA processes shall document security administration including managing role and End-User database permissions and in accordance with the County security policies. Contractor shall perform database restores when required.

Contractor shall define, document, and execute database creation, configuration, upgrades, patches, refreshes, database system-level changes, schema changes, and definition requirements for applications. Contractor shall maintain documentation for portfolio applications database instance parameters and system settings and manage them across like instances when required during the application change process. Contractor shall provide and execute proactive database performance and tuning scripts and monitor database performance for optimal performance.

Contractor shall implement and manage County-approved appropriate database management tools across application portfolio database instances. Contractor shall capture performance metrics and historical data for trending and reporting. Contractor shall use Oracle Enterprise Manager to manage the Oracle/UNIX enterprise applications. In conjunction with Oracle Enterprise Manager, Contractor shall use the Applications Performance Management (APM) tool to provide a full 360-degree view.

Also, Contractor shall identify and resolve locking conflicts, latch contention, and rollback requirements for database instances and implement database monitoring tools that generate automatic Service Desk trouble tickets for incidents.

Contractor shall provide technical assistance and subject matter expertise to application developers and third-parties. Contractor shall provide data dictionary knowledge, End-User data assistance, data warehouse metadata definition, and data mapping.

Contractor's DBAs shall patch database software as approved and manage database communication software configuration, installation, and maintenance. They also shall provide database storage management and cleanup activities, backup schedules, retention periods and levels, and execute backups and recoveries that adhere to the County's policies.

Contractor's DBAs shall provide database capacity management and availability management, maintain database storage allocation, file systems current usage, and capacity. Contractor shall conduct database installation, de-installation and administration, testing, copying, and security and database server management, as needed and provide administrative account support that shall include provisioning and de-provisioning. Contractor shall create and provide system monitoring and documentation, maintain transactional logs, and backup as scheduled. Finally, Contractor shall provide operational support for the County's public and private cloud databases.

7.3. Application Development Services

- Deployment plan for resources and use of facilities

Staff shall be located at the Contractor's Rancho Bernardo site, El Paso, TX and Pontiac, MI.

7.3.1.1. Process and Procedures

- Applications Development Services

Contractor shall reach out to Third Party providers who can deliver quality apps projects on time and within County budget. Contractor shall work to include applications providers in Contractor's outreach process that currently includes more than 20 different vendors. Contractor shall also reach out to Disabled Veteran Business Enterprises (DVBE) and give them the opportunity to provide services.

Contractor shall continue to work with the County to use COTS and third-party applications where appropriate. On a per project basis, Contractor shall reach out to third-party providers as resources and expertise is needed. If the County has a requirement for a specific or unique solution, Contractor shall engage with those application providers as described in the "Procurement of Third-Party IT Solution via the ITO" process referenced below.

Contractor shall provide third-party vendors access to the development and test (Dev/Test) environments.

Applications Development Services shall be conducted either on a time & materials basis using Resource Units defined in the Agreement (e.g., labor hours based on the Labor Categories) or on a firm, fixed price basis, at the County's option. A fixed price for Applications Development Services shall be based on defined statements of work, and may include warranty services as negotiated and agreed-upon by the parties.

There shall be two types of estimates for Applications Development Services:

1) Budget Estimate (BE) – A BE shall be generated by Contractor upon County request. The BE shall establish a range, or rough order-of-magnitude estimate based on a statement of work, for County budgeting purposes. Preparation of a BE shall be a non-billable task.

2) Service Request Project Estimate – A Service Request Project Estimate shall be generated by Contractor upon County request. The County shall provide a detailed statement of work and requirements to accompany the request. The County does not anticipate significant overhead to generate estimate, given that the statement of work and requirements are already complete, but solution design, detailed one-time and on-going cost estimates (including the cost and time to bring a development project into the Applications Portfolio), resource breakdowns, and impact analysis shall be billable. Depending on the size of the project, a Service Request Project Estimate may be covered by Service Levels once the project is approved by the County.

When procuring Application Development Services:

1) The County develops a statement of work, either using its own resources or by leveraging Contractor resources using the approved Labor Categories. The result is a specific statement of work to meet the County's business requirements.

2) The County determines the appropriate procurement vehicle, either using the Agreement or pursuing an alternate path (e.g., County Purchasing and Contracting).

3) If the County decides to leverage the Agreement, it may:

   a. **Contractor Estimate:** Issue a Service Request to Contractor either soliciting a time and materials proposal (using the Resource Unit labor rates) or a firm, fixed price proposal. Upon County approval, Contractor shall (a) use its own resources to deliver these services or (b) use its network of Subcontractors to execute the work;

   b. **Request for Information (RFI):** Issue a Service Request to Contractor to conduct a market scan, to be performed by the Acquisition Manager, using the approach set forth in the Standards and Procedures Manual to identify potential solutions and/or vendors. Contractor shall conduct a market study and provide the results to the County for review. Services performed by Contract and Acquisition Management Services resources shall be covered by the Cross-Functional Services Framework Resource Unit. Assistance by Contractor Applications resources for the purposes of the evaluation shall be billable in accordance with the applicable labor rates upon County approval;

c. **Pre-Approved Vendors Request for Proposal (RFP)**: Submit a Service Request to Contractor and direct Contractor to facilitate a competitive procurement process among a list of pre-approved vendors that have a master agreement with Contractor allowing for rapid execution of Statements of Work ("Pre-Approved Vendors"). Contractor shall provide to County a list of Pre-Approved Vendors as part of Schedule 5.

Contractor shall post County requirements from the Service Request (mechanism to be determined, likely a SharePoint site), alert its Pre-Approved Vendors of the pending opportunity, and require responses within a specific timeframe, which shall be communicated to the County. Pre-Approved Vendors shall be required to respond to Contractor within the stated timeframe with a firm fixed price proposal to complete the Service Request. Contractor shall review the responses and share qualified responses with the County along with a recommendation to proceed (or not). Contractor shall work with the County to select the pre-approved vendor that offers the best value to execute the Service Request based on criteria agreed upon in advance of the competitive process. Upon County approval, Contractor shall contract with the selected pre-approved vendor to execute the Statement of Work (services requested). If this process is used, the Resource Unit labor rates do not necessarily apply for the pre-approved vendor proposal, since the competitive procurement process among Pre-Approved Vendors provides a mechanism for fair and reasonable pricing, assuming multiple offerors. The proposals from the Pre-Approved Vendors shall be submitted to the County at no additional cost to the County; and/or

d. **Request for Proposals (RFP):** Submit a Service Request to Contractor and direct Contractor to facilitate a competitive procurement process among third-party vendors, to be performed by the Acquisition Manager, using the approach set forth in the Standards and Procedures Manual. Contractor shall work with the County to select the vendor that offers the best value to execute the Service Request based on criteria agreed upon in advance of the competitive process. Services performed by Contract and Acquisition Management Services resources shall be covered by the Cross-Functional Services Framework Resource Unit. Assistance by Contractor Applications resources for the purposes of the evaluation shall be billable in accordance with the applicable labor rates upon County approval.

Contractor shall document the foregoing procedures in more detail in the Standards and Procedures Manual.

Pre-Approved Vendors List Management

Contractor shall add Pre-Approved Vendors that (1) are existing vendors that have requested to be Pre-Approved Vendors, (2) have agreed to terms and conditions and (3) have provided proven value to the County. Additional Pre-Approved Vendors shall be added from the larger group of Contractor providers with which Contractor has established master agreements and that provide services applicable to the County. Contractor shall also use all reasonable efforts to add vendors to the Pre-Approved Vendors list in response to County requests requiring frequently used niche skillsets.

Contractor shall maintain no fewer than five (5) Pre-Approved Vendors who are eligible to propose on County applications work. Contractor shall choose vendors based on specialty skills with specific technologies (ex: Captiva, SharePoint) or general skills required by County projects (ex: Project Management).

Contractor shall add Pre-Approved Vendors as identified and compliant; Contractor shall post the current list of Pre-Approved Vendors on the Service Portal

After CY1, Contractor shall add and maintain Pre-Approved Vendors based on County demand as follows:

Number of Service Requests	Minimum Number of Pre-Approved Vendors
< 15	Five (5)
15 - 25	Seven (7)
26 - 50	Ten (10)
51+	Fifteen (15)

At the end of each Contract Year, Contractor shall notify County if Contractor is unable to meet the minimum number of qualifying Pre-Approved Vendors and shall provide County a recommendation on next steps to meet or modify the County’s requirements.

- Solution to meet the requirements

Contractor’s solution shall use an established Contractor application development framework plan, build, operate to meet deliverables requirements. This framework accommodates Agile, Iterative, and Waterfall methodologies, making sure roles and responsibilities are defined, governance processes are in place, and the work follows a structured approach to achieve its objectives. Contractor’s applications team shall tailor the framework.

Contractor’s application development framework shall provide a delivery and governance framework covering all aspects of IT-enabled business change. The framework spans the full delivery life cycle, from application development planning through operations. Security shall be managed during the life cycle of the application, from discovery through operations.

Development Process

Contractor’s development processes shall follow SDLC, using Agile, Iterative, and Waterfall methodologies as appropriate.

Each project shall:

- Engage key stakeholders
- Identify the business, security and DR, and business continuity and planning requirements
- Analyze the requirements from internal and external perspectives
- Prioritize and select projects that shall be included in the program scope.

For gathering and identifying requirements, Contractor shall leverage the Requirements Determination Process (RDP) that contains five major components: plan/manage, obtain, understand, validate, and evaluate, as delineated in following table. Contractor shall obtain, understand, and validate components make up the core of the RDP. Contractor shall execute these components multiple times, once for each set of requirements.

Five Major Components – Requirements Determination Process

COMPONENT	PURPOSE/ACTIVITIES
Plan/Manage	Contractor builds the plan that Contractor shall follow throughout the process and manage overall execution of the RDP.
Obtain	Contractor collects the information for the business, technical, security and DR, and business continuity planning needs of the County. Contractor shall store the information Contractor obtains for later retrieval and traceability.
Understand	Contractor shall analyze the collected information to make sure Contractor has a good understanding of the requirements. Contractor then evaluates the statements for consistency, completeness, and appropriateness. For each statement, Contractor shall establish traceability and validation criteria and perform RCA.
Validate	Contractor shall confirm a mutual understanding of the implications of the requirements with the County and Contractor SMEs, who shall build and implement the solution.
Evaluate	Contractor assesses how well the process worked and determine the effectiveness of the techniques and the requirements statement. Contractor shall work with the County to prioritize the requirements and establish a roadmap.

During design, project details shall be defined to align with the County's strategic direction.

Requirements are captured and more detailed views of the "As Is" and "To Be" states shall be developed.

For existing applications, Contractor shall review the current state of the architecture and identify the impact of the solution as well as alternative solutions. Contractor shall notify the County of any changes that impacts the current architecture so a decision on solution options can be made early in the development cycle. Contractor shall also conduct industry research to identify any COTS product solutions that may meet the requirements.

The application architecture and its impact shall be reviewed with the County to provide a better understanding of the changes and a solution design document shall be created to document the solution with changes to the application, database and the infrastructure as needed. All design features as well as changes to data models and configurations shall be documented. Detailed procedures to migrate data to the new data models shall be defined.

Once requirements are defined, Contractor shall expeditiously notify external applications providers and invite them to provide a bid for the work.

After selection of an applications provider (Contractor or a third-party), the provider shall develop a detailed project along with an applications roadmap. The following describes various phases and deliverables of the project.

Deliverables for the assets and align phase include:

- High-level application solution design
- Application architecture
- Future roadmap
- High-level project plan.

When the project is implemented, the handover to M&O is executed to include documentation, training, and updated Service Desk scripts.

The project plan shall include details of the application development, testing, integration, and implementation schedules. Contractor shall use Contractor's risk management processes to mitigate risks early in the process. Contractor shall provide detailed project and cost information to the County, and all changes to the plan and cost Contractor shall follow the change management processes established by the County.

Deliverables for the design phase include:

- Detailed design document
- Update architecture document
- Detailed project plan
- Risk and mitigation strategies
- Detailed project cost estimates
- Updated requirements document.

The develop phase shall produce the application code according to the application design. The primary deliverables are application code and test scripts and, when needed, a pilot run of the application. Key activities include:

- Application code development and test
- Gain authorization from the County to proceed to implementation.

During this phase, the needed Dev/Test environments shall be created. As new applications that are targeted to run in the MPC are developed, the Contractor team shall request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team shall then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team shall submit a service request to de-install the MPC infrastructure for that application. The team shall decommission all of the application components and infrastructure resources for the application environment being retired, and shall release any licenses through Asset and Configuration Management. If the environment is a Dev/Test environment, the request shall specify whether the environment shall be permanently decommissioned or put into cold storage. If the latter applies, the image shall be preserved on the SAN storage and held in an online inventory, but its compute resources released. Otherwise, all resources shall be released.

Contractor shall not use the MPC for production use, unless an exception is authorized by the County Technology Office. From a Resource Unit (RU)/billing perspective, only moves into and out of MPC for production application environments trigger activity: new RUs are added to billing at the point a production environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved (the billing change shall not wait for the decommission process to complete). If a production application moves from a traditionally hosted environment to, the old RUs are removed, and new ones take effect at the point when the MPC environment becomes available for County use. The County shall not be billed for both sets of resource units. The same approach shall apply in reverse if an environment moves from MPC to a traditional environment.

Additions and removals of Dev/Test environments into and out of MPC may trigger a slightly different RU action. Additions of new applications to MPC “draw down” on the pool of available resources. If the application is very large, such that its requirements exceed the capacity available (this scenario shall be the exception rather than the rule), Contractor may need to acquire more resources to expand the cloud. In most cases, the resources shall be available, and the environments shall be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool shall not trigger a change to RU billing. Moves of existing Dev/Test environments into and out of MPC shall have no billing impact.

During this phase, application developers shall implement the application according to the functional specification and application architecture. The developer shall follow Software Development Lifecycle Standard County process and standards to code, build, and deploy. The configuration changes shall be documented and shall become part of the deployment package. The technical lead shall coordinate integration testing with the developer in the development test environments. The designated testing team shall also perform QA testing and End-User acceptance testing (UAT) and partner integration during this phase.

During the development phase, additional risks may be identified. Contractor’s Project Manager shall use the Risk management processes to mitigate these risks. Changes to the project plan and cost shall follow the defined change management processes.

Contractor’s project manager shall coordinate with the County to obtain approval for UAT and deployment to the production environment.

Deliverables for the develop phase shall include:

- Application code
- Test scripts, including test plans for the independent test team
- UAT results
- Risk and mitigation strategies.

Implement

After gaining the approval from the County using the successful UAT results, Contractor’s deployment team shall prepare the release package for deployment to production. A deployment plan shall be created in coordination with the application users, the integration touch points and the M&O team. The deployment instructions including the configuration details and the data migration steps shall be outlined and validated before deploying the application.

Deliverables shall include:

- Deployment Plan
- Deployment Package
- Third-party cross-training of Contractor staff to perform required M&O activities, as required.

Manage

Once the application has been deployed in production, Contractor shall provide production support under the Applications M&O Services framework. The project team shall load all documentation, such as the architecture and design documents and the deployment package instructions, to the DocVault site for the M&O team to review. An initial hand-off session shall be provided to the M&O team so that the developers become aware of the changes.

The project team shall coordinate and work with Contractor resources to perform market research and technical trends, and provide new products and services and third-party solutions that may be applicable to the County. The team shall work with the County to evaluate these services and make recommendations. The team's reach-back into Contractor's quality management office shall facilitate the process to provide recommendations on changes to SDLC, leveraging ITIL practitioners and their relationships with Software Engineering Institute (SEI).

High Level Requirements

Alignment with IT strategic plan and roadmaps: Contractor understands the County's strategic plan and transformation roadmap and shall ensure that all technology, innovation, reengineering, and business processes align. The development process shall follow standards and guidelines published by the County's IT governance bodies and the architectures shall comply with County-approved enterprise architecture(s), as well as abide by County security policies and models for system architecture and technology.

Contractor's approach shall begin with analyzing requirements and constraints. Analysis of functional inputs shall inform the business architecture view, which describes the high-level functional composition of the system and shows various actors, usage scenarios, and interdependencies among functional modules. After the first phase of high-level design is complete, the architecture artifacts shall be submitted to County staff, as required, for review and approval. The outcomes of the review shall be addressed by further aligning the architecture with the County's business and technology direction and resubmitted for approval.

Contractor shall recommend updates and revisions to architecture and/or configuration change designs in response to changing requirements, emerging technology, and other activities such as vulnerability assessments and performance analysis. Contractor shall monitor industry trends and best practices and make recommendations to the County for other inclusions in the technology roadmap.

The software development process shall follow the established SDLC process and generate documentation as required by the size and complexity of the project. As required, Contractor shall produce architectural design documents in compliance with the County's requirements and alignment with the County IT strategic plan and applications roadmaps.

Integration with existing data and Applications.

Contractor architects, engineers, developers, and operations support teams shall work in concert to facilitate new components introduced into the environment that are able to function as designed without negatively impacting existing systems or County users.

IT standards, guiding principles, architecture bricks and patterns. Contractor follows all applicable standards and compliance requirements of the County and shall maintain and support applicable CMMI, ITIL, and ITSM standards and industry best practices for the delivery of IT services.

Using Contractor's application development framework, Contractor or a third-party shall design the solutions for the requirements. Contractor shall follow County's IT standards, guiding principles, and architecture bricks. Any deviations shall be identified early in the development cycle.

Planning and Standard Setting: For planning purposes, the Contractor Program Office shall provide budgetary estimates as required and follow standard change control procedures.

Contractor shall follow applications standards and work with the County to refine, improve, and modify as required. Contractor shall use Contractor's Program Quality Office to validate best practices, tools efficiency, and process improvements.

System Documentation. Contractor shall maintain the documents for the County program, with a sustained effort to improve timeliness and accuracy.

Cross-Framework Integration. All of the dependent applications, which are part of the impacted framework(s), shall be identified as stakeholders for developing the new requirement.

Contractor staff shall collaborate with the other framework teams to develop an interface control document, which shall become the guide to perform the integration between the frameworks.

Contractor's independent testing team shall perform integration testing and, where possible, use service virtualization tools to test interfaces.

ITIL/CMMI Practices. Contractor shall operate the County environment using ITIL and CMMI best practices. The Contractor ITSM community provides knowledge, best practices, and lessons learned to everyone supporting the County. Contractor shall leverage these unparalleled qualifications when bringing ITIL and CMMI-based processes to the County and recommend any changes to existing policies and procedures.

Standards

Contractor shall follow County's IT standards, guiding principles, and architecture bricks. Any deviations shall be identified early in the development cycle and communicated to the County. Contractor shall follow existing applications standards and work with the County to refine, improve, and modify as required.

Transition. Contractor's deployment plan shall include a strategy to migrate the application into M&O services. Upon implementing the project in production, Contractor's development team shall complete transition to the M&O team in an orderly, controlled manner that includes reviewing processes and outcomes, capturing lessons learned, and creating formal closure documentation.

- Processes in solution including year-to-year continuous improvement

Contractor shall leverage Agile, Iterative, and Waterfall methodologies as needed for each project. The methodology selection shall be discussed with the County and the necessary process shall be executed based on the needs of each project.

As members of the PMI and ITIL communities, Contractor shall provide training for resources, including acceleration programs for the PMP, CAPM, SPI, ITIL, and other disciplines. Contractor participates in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, State/ Local Government/Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice. In addition, Contractor shall monitor industry standards for emerging methodologies and discuss Contractor's findings with the County.

Processes, procedures and use of tools in new systems planning, SDLC, project management, testing (including methods to engage the County) implementation (including methods to engage the County), post-implementation evaluation/review and transition (including transition support for newly implemented applications). Processes followed by Contractor organization that shall minimize disruption to business operations.

Software Development Lifecycle Methodology and Processes

Contractor shall perform full software development lifecycle (SDLC) process activities for developing and implementing new systems and major scope enhancements to existing and evolving systems.

Contractor shall comply with its governance and enterprise architecture principles as well as its procedures.

For each development project, Contractor shall work with the County's project sponsor to create a project plan. The plan shall detail the customized development approach to deliver the desired results with the best quality in the shortest time. Contractor shall provide a proven development model that are widely practiced in the industry and that Contractor has used previously at the County and on other successful projects.

The following table list software development models along with the general characteristics of each and the type of projects for which each model Contractor shall provide:

Application Development Models

DEVELOPMENT MODEL	CHARACTERISTICS	SUITABLE FOR PROJECTS WHEN –
Agile	• Software is developed and tested in short iterations (1 to 4 weeks) • Adaptive • Iterations are usually time-boxed to limit risk • Software is the principal measure of progress, with less emphasis on intermediate artifacts • Face-to-face communication is preferred to documentation	• Requirements are not well known but can be evolved through short cycles • The project team is relatively small so that developers and customers can easily communicate and incorporate feedback into the next interaction
Waterfall	• Sequential process that flows through requirements capture, analysis, design, coding • Plan driven • Predictive • Low risk • Expected results clearly defined up front	• Requirements are well defined up front and changes are expected to be minimal • System reliability is critical • Documentation requirements are high

DEVELOPMENT MODEL	CHARACTERISTICS	SUITABLE FOR PROJECTS WHEN –
	• Generally, artifact intensive (models, plans, documentation)	• Project team is large and incorporates many disparate organizations

Contractor's applications team adheres to County procedures that can be applied to Waterfall, Agile, or, alternatively, Agile/Scrum.

Contractor shall use the following activities that are common to nearly all projects:

- Business Modeling
- Requirements
- Analysis and Design
- Implementation
- Testing
- Deployment
- Configuration and Change Management
- Project Management
- Environment

Project Management

Overall governance of development projects shall be managed by Project Management. Contractor's ITIL-aligned project management methodology supports recognized industry standards, including the CMMI Institute's Capability Maturity Model Integration (CMMI), Projects IN Controlled Environments (PRINCE2), and the Project Management Institute's Project Management Body of Knowledge (PMI PMBoK) Guide.

Contractor shall use a proven set of tools (like HPE's Project and Portfolio Management Center (PPMC)) to plan, budget, and track cost, scope, and schedule performance data. Contractor shall engage the County in each step of the system development process—from evaluation to deployment.

Contractor shall provide a Service Portal that include access to the County on Contractor service level performance, project schedules, and cost.

Testing

Contractor shall leverage the Contractor's Enterprise Testing (ET) Methodology to plan, develop, and conduct an integrated Test Program. The methodology shall provide County visibility, traceability, and accountability in requirements management and verification; it shall also provide risk identification, management, and timely resolution in support of the County development and maintenance activities, as shown in

Using Contractor's ET Methodology—a comprehensive framework that provides the structure, processes, tools, and templates—Contractor shall align to the County SDLC.

Contractor's test team shall conduct the Test and Evaluation (T&E) program, including managing the creation of test plans and procedures, testing, and developing test reports; communicate the result of testing and recommendations to the team and to the client; and provide input to Contractor's Program Manager on cost, schedule, and staffing for meeting requirements in this area.

Contractor shall prioritize high-risk, high-value business requirements and concentrate testing activity on those requirements to minimize risk and deliver the most value to the County for the application implementation. Contractor shall set the testing strategy based on the value of a business function as well as the potential for failure and the associated risk. The testing strategy applies the highest levels of test coverage to the highest-risk, high-value functions.

Contractor's risk-based, requirements-driven testing has the following components, shall be executed iteratively:

- **Ambiguity Analysis –** Contractor shall conduct an ambiguity analysis to make sure that the requirements document is deterministic (with randomness removed), unambiguous, correct, complete, and testable. Contractor shall systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize inconsistencies and maximize requirements clarity.
- **Risk Analysis –** Contractor shall systematically analyze risks in those requirements to reduce chances of misdirected or incomplete test coverage, with focus on isolating and mitigating the most critical risks first—those that most negatively affect the highest-priority aspects of an application or system.
- **Systematic Test Design –** Contractor shall use methodical activities focused on managing and mitigating risks, Contractor shall apply test design techniques to plan, choose, and develop the most effective tests to verify from the bottom up to integrated functional areas and interfaces within the complete system for operational configurations and environments.
- **Requirements Traceability –** Contractor shall provide throughout test development and execution, Contractor use a Requirements Traceability Matrix (RTM) to comprehensively depict test coverage and keep testing focused on high-risk, high-priority requirements.
- **Testing Metrics Collection/Reporting –** Contractor testing reports offer ongoing insight into testing progress, coverage, and defect resolution; they offer timely opportunities for acting to mitigate risk before it causes irreversible harm.
- **Testing Close-Down Activities –** While testing ends with all tests executed, all defects resolved, and a system unquestionably ready for release, defects can outlast time and budget limits. Contractor shall focus on satisfying high-risk, high-priority requirements first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements, as agreed upon in the Test Plan.

Contractor's applications group shall use the following tools from Contractor's Application Lifecycle Management (ALM) tool suite: the HPE Quality Center tool for test management and tracking, HPE Unified Functional Test for automated testing, and HPE Performance Center for performance testing. Contractor shall use these tools to manage and develop a series of test scenarios and test cases that test the entire solution for functional and performance quality. Based on the broad scope of Contractor's testing and tools, Contractor shall use automated and manual test scenarios and cases to fully test the solution. Contractor shall manage the test scenarios and cases with the HPE suite of testing products and then link and trace them to the approved requirements.

Implementation

After Test, Installation, and Validation phases have been successfully completed, the implementation process continues with a final review of success factors, associated risks, and mitigation strategy. All of the primary technical functions shall be documented and targeted, making certain that the applications development team and the County business owner agree with the decision to go to production. As documented in the pre-application cutover phase, each functional area shall be reviewed for completeness, functionality, and readiness.

Contractor shall mitigate risks to integration of systems by applying Contractor's consistent, repeatable system integration and project methodology that provide effective communication, coordination, and collaboration with the County, that shall result in a fully integrated solution.

Contractor shall develop a back out plan for each implementation to provide for rapid rollback to the original state if required. Whenever possible, the source system remains up and running until Contractor is sure that the workload has migrated successfully. This approach provides a fully redundant contingency; immediately after implementation, Contractor's Applications Development team shall test the functionality in the production environment to make sure County users shall not experience any disruption.

Transition to Application M&O Services

Upon successful implementation, the Contractor's application M&O staff shall provide support for the production application. Prior to production cutover, the Applications M&O team shall receive cross-training and documentation to provide a smooth transition from the development team. The development staff shall also review with the M&O staff any changes to the design and deployment document as well as the test results.

Application demand management methodology

Contractor's ITIL-aligned demand management methodology uses frequent communication with the County Technology Office to maintain alignment with the County's strategic priorities and schedules for new or modified application deployment.

Demand Management shall be approached with two methods; PPMC Demand Management module and Demand Growth & Innovation

Demand Growth & Innovated Solutions

The Business Analysts (BA)/Solution Architecture (SA) Service Center shall work with the department to ensure their demands are being managed. BAs shall assist the County in identifying and prioritizing future demand. Embedded with County departments, BAs shall work closely with the County users and have a solid understanding and the ability to articulate the departments business needs. BAs shall detect prospects for driving business innovation, aligning IT initiatives with business goals, to the SA and CTA. In turn, the SA/CTA shall work with the CTO to determine which technologies may be required to meet the business need. From that determination, the applications team shall forecast demand by department, technology, and timeframe.

Contractor shall host road mapping sessions including white board activities to better understand business demands, integrate with Contractor's innovation process and provide technology showcases on a regular basis as determined by the County and Contractor. The objective is to define a multi-year roadmap (over 5 fiscal years) to improve departments' ability to plan for change and influence IT direction in the overall County IT environment. The BA/SA partnership is key for defining their architectural/business road maps. The roadmap shall consider four key components:

- High level County/business objectives
- Technology/Vendor Lifecycle Roadmaps (e.g. Windows/Oracle, SQL)
- KPIs to measure roadmap progress
- Department PAIDs and projects

Contractor shall hold these sessions every 6 months or as otherwise determined by the County and shall review road maps, historical trends and map out business group's strategic plans and adjust road maps to meet the technology and business demands.

Contractor demand management practice shall facilitate staff planning, working with the County to identify slowdowns, provide a predictable forecast for budgeting and keep the business move in the right direction.

Demand Management with PPM

The Contractor's application demand management tool shall be HPE's PPMC Demand Management module. HPE PPMC consolidates, prioritizes, and fulfills the strategic application projects activities so the County can redirect activity based on demands.

The PPMC tool lets Contractor consolidate and prioritize the applications requests and focus on the highest-priority County initiatives.

Because the PPMC Demand Management module captures all IT requests, it enables County stakeholders to have a comprehensive picture of past, present, and future IT demands, grouped by demand category.

The PPMC Demand Management module processes a request based on the best-practice process and business rules for that type of request, after each request is captured. The process behind each request is modeled, automated, enforced, and measured. Automated, out-of-the-box, best-practice processes—including proposed projects, application-related enhancements, project scope change requests, non-project related requests, and others—are easily configured to support the County's specific best practices, using a drag-and-drop process modeler.

The module helps responding to new demands and changing priorities by redeploying resources and provides the automated processes and data necessary to effectively manage status, service levels, and trends. Web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels shall be updated automatically as each request is processed.

Business rules define when to send notifications so the PPM module can monitor processes in real time and alert the County and Contractor's applications team when something needs attention.

When priorities change, cycle times may be exceeded, or other requirements possibly may not be met, PPM can trigger an escalation process. With this level of visibility and control, Contractor can focus on the highest-priority requests and know quickly whether a project may be in jeopardy.

How HPE PPM Demand Management Works

Each request type shall have an associated workflow, which specifies the process for reviewing, evaluating, prioritizing, scheduling, and approving the request. Based on the workflow, the Contractor reviewer shall assign the request to a person or team for scheduling and delivery. Notifications defined as part of the process shall be activated at any step to indicate work that needs to be done, has not been done, or is being escalated.

With online access, Contractor managers shall assign tasks, and developers can view and work on tasks assigned. Service levels are updated in real time, and changes are captured for a complete audit trail. Contractor shall link the module to the new Service Portal described.

Contractor shall provide the following key features and benefits of PPM Demand Management:

- **Shared demand repository**

- **Unlimited demand categories**
- **Demand scheduling and prioritization**
- **Drag-and-drop process modeling**
- **Complete audit trail**

Contractor's approach for performing system analysis and design for major new development projects and enhancements. Describe how Contractor expects the County to be involved in the analysis and design process.

Contractor shall work collaboratively with the County during the planning, analysis, and design phases of development projects. Contractor shall include the following activities that Contractor shall perform iteratively throughout the delivery life cycle. Contractor shall adhere to the County Standards and Procedures applicable to all applications development projects.

Collaborative Planning with the County – Analysis and Design

Upon receipt of an approved request, Contractor shall kick off the project by conducting a series of workshops with the County project sponsor. Contractor's team's focus during the planning workshops is to facilitate collaborative dialogue with the County on design of the new system. Contractor's expectation is that the County product owner shall describe the intended result so Contractor's team can understand the requirements, begin to design the architecture, and apply technical standards.

During these workshops, Contractor shall discuss "End-User stories" that encourage the County to visualize the new system as deployed. Analysis of the new system shall include realistic assessment of anticipated improvements, potential limitations, and possible risks. Contractor also shall discuss system business rules needed to facilitate continuity from the existing process to the new system. **Error! Reference source not found.**Contractor shall build a roadmap and next steps with the County that sets realistic target dates for solution design, development, testing, and deployment. The roadmap shall define the County's role throughout the development process.

Contractor's approach allows the County to continue to provide design input throughout Contractor's iterative processes, keeping the new system development aligned to County objectives.

Contractor shall maintain SDLC documentation as the project progresses. This shall include documentation of the County's priorities, the solution design and its characteristics and features, results of the collaborative analysis including risk assessment, and the improvements anticipated upon deployment and all approved changes. Based on the planning workshop discussions, Contractor's team shall refine and document the functional and nonfunctional technical requirements and submit them for County approval.

Cloud and E-commerce solutions. Contractor experience implementing E-commerce and cloud solutions.

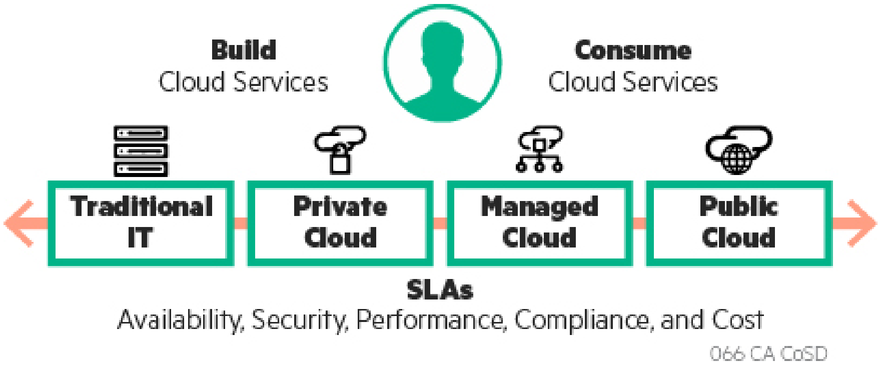
Cloud Services

With the planned consolidation to the Tulsa data center, Contractor shall take this opportunity to move the current Dev/Test application infrastructure from a well-performing traditional hosted environment to a more agile, hybrid Managed Private Cloud (MPC) for compatible platforms, and retain the traditional hosted environment where necessary for applications that are not initially cloud compatible. The MPC environment shall be a highly standardized environment with high redundancy and high availability for both infrastructure and applications to eliminate single points of failure. Moving to MPC provides benefits of streamlined server provisioning, enabling Contractor to provision, scale, and de-provision virtual servers in hours instead of days. This shall also include tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance and provides the foundation for the County to take advantage of additional public cloud services. Contractor shall work with the County to identify production applications that are candidates for the MPC environment.

In partnership with AT&T, Contractor shall provide virtualized services for the County. Contractor's network is designed to provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," Contractor's network shall enable any device managed or unmanaged to be evaluated, authenticated, and allowed policy-based access.

Contractor's solution's End-User-friendly portal shall result in quick adoption, and provide state-of-the-art software for cloud service catalog presentation, automation, management, and orchestration. HPE's Cloud Service Automation (CSA) Portal platform is the End-User entry point into the Cloud Consumer Portal. Users can view service details and subscriptions through an easy-to-use self-service portal.

Full Suite of Cloud and Cloud Broker Services



066 CA CoSD

Contractor's cloud solution shall enable delivery of IT resources as "services"—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—to consumers using ITIL-based management and operational support processes through a web-based, private Cloud Consumer Portal. Contractor skilled resources shall provide setup, configuration, and ongoing management of the private cloud, so applications development staff can more effectively complete projects.

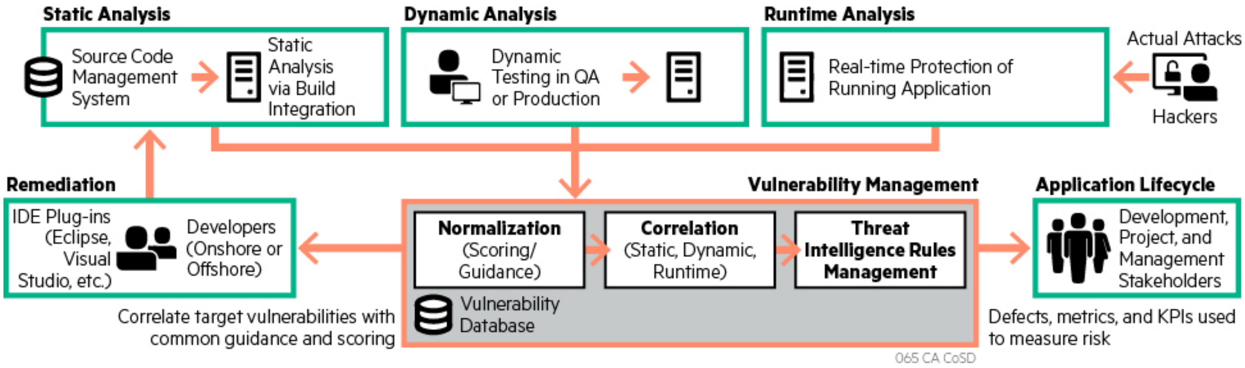
Contractor's CloudSystem shall enable Contractor's development team to build and manage services across private cloud environments on a simplified, integrated architecture:

- Intelligent automation; application-to-infrastructure
- Complete service life cycle management—from provisioning to monitoring to retirement/de-provisioning
- Supports multi-hypervisor, multi-operating system (OS), and heterogeneous infrastructures – now including Kernel-based Virtual Machine (KVM) and Hyper-V support
- Pre-packaged service design tools – HPE Cloud Maps, which are pre-configured and standardized workflow templates for infrastructure deployment, application deployment, and life cycle management;
- Out-of-the-box bursting capabilities broker service delivery across multiple clouds from a single, integrated point of control
- Built on proven and market-leading HPE Converged Infrastructure and HPE Cloud Service Automation (CSA). Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. Contractor Server Automation software enables Contractor to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with Contractor IT configuration standards.

Security

Contractor's cloud solution shall provide capability to perform Static Code Analyzer (SCA). This service focuses on implementation of the Static Analytics, Remediation, and Vulnerability Management of the architecture in the following figure.

Essential Building Blocks of a Mature, Secure SDLC for Cloud Services


Static Analysis
Source Code Management System
Static Analysis via Build Integration
Dynamic Analysis
Dynamic Testing in QA or Production
Runtime Analysis
Real-time Protection of Running Application
Actual Attacks
Hackers
Remediation
IDE Plug-ins (Eclipse, Visual Studio, etc.)
Developers (Onshore or Offshore)
Vulnerability Management
Normalization (Scoring/ Guidance)
Correlation (Static, Dynamic, Runtime)
Threat Intelligence Rules Management
Vulnerability Database
Application Lifecycle
Development, Project, and Management Stakeholders
Correlate target vulnerabilities with common guidance and scoring
Defects, metrics, and KPIs used to measure risk
065 CA CoSD

Contractor shall provide a, short-track implementation into the County environment that shall result in a scan of the target application. This shall enable Contractor's team to accomplish the following:

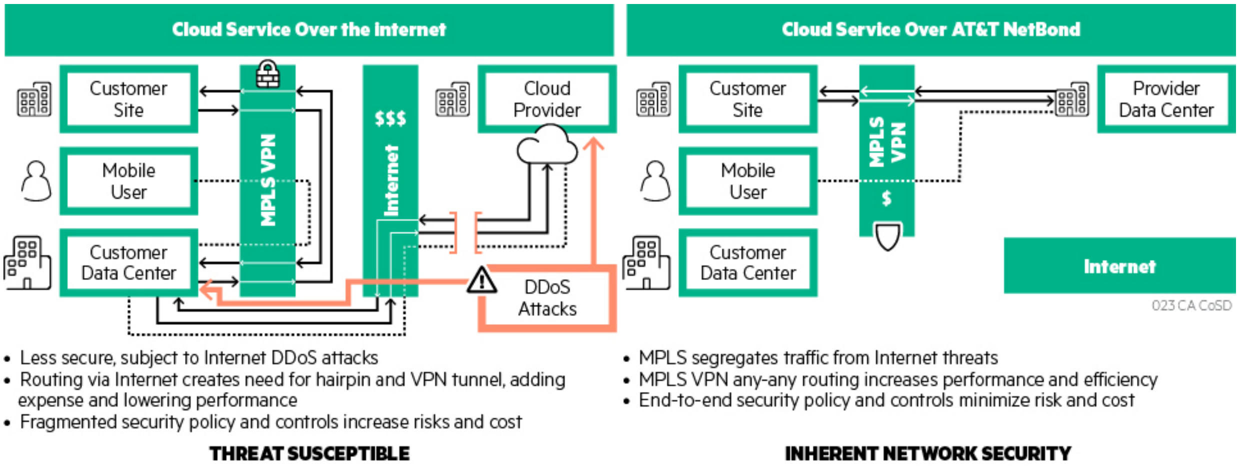
- Produce SCA scans
- Triage scans results to identify and prioritize security vulnerabilities
- Incorporate the Contractor solution for the County into the development process

Embedding Contractor's solution within the software development lifecycle shall enable secure development practices and shall keep applications protected from external threats.

In the background, Contractor's network security is built on AT&T cloud security.

The following figure shows the AT&T NetBond as a basis for cloud services for the County.

Cloud Service over AT&T NetBond



- Less secure, subject to Internet DDoS attacks
- Routing via Internet creates need for hairpin and VPN tunnel, adding expense and lowering performance
- Fragmented security policy and controls increase risks and cost

- MPLS segregates traffic from Internet threats
- MPLS VPN any-any routing increases performance and efficiency
- End-to-end security policy and controls minimize risk and cost

Contractor avoids the security risks of the typical cloud service over the Internet by providing end-to-end security with NetBond.

HPE Cloud Service Automation (CSA) goes beyond traditional IT provisioning; it increases agility and reduces costs. This solution shall offer the following:

- Leverages a modern, easy-to-use self-service portal with an intuitive shopping cart experience for ordering infrastructure and application services across both private and public cloud environments.
- Enables an open, heterogeneous, and extensible architecture supporting OpenStack-based cloud standards, with multi-hypervisor, multi-vendor hardware support that avoids the pain of vendor lock-in.
- Embraces existing automation assets in a highly automated cloud lifecycle management platform that uses an enhanced orchestration engine.
- Designs and orchestrates full-stack services with topology service designs for faster time to value
- Stages complex multi-tier applications with sequential service designs
- Gains enterprise-grade service management with a highly available architecture, providing informed, transparent IT service delivery for secure and compliant services.
- Creates an IT service control point, enabling hybrid IT management across the expansive HPE Helion portfolio of private, public, and hybrid cloud services.

The solution features an open, extensible architecture that supports HPE and third-party management tools, enabling Contractor to quickly adapt to changing business requirements while supporting heterogeneous IT environments.

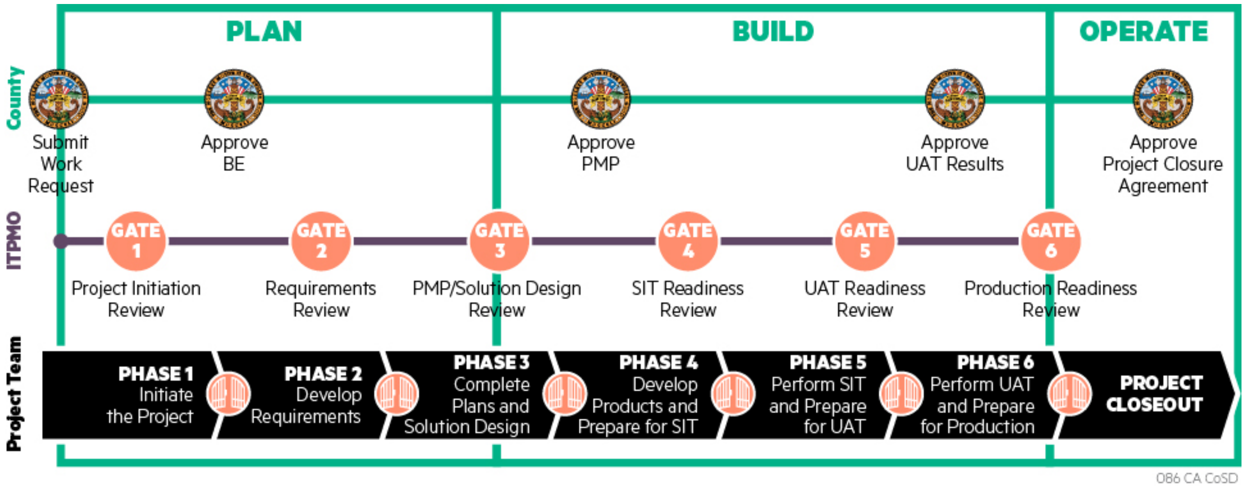
Waterfall and agile development

Contractor shall use Waterfall or Agile approaches based on best fit for the project.

Waterfall Approach

In Waterfall life cycles, each phase (Define and Analyze, Design, Build, Test, Release, and Deploy) is typically executed sequentially, possibly with overlap but with little or no iteration. Contractor shall use Waterfall life cycle development for projects that require a Waterfall approach to deliver business applications or to implement major application enhancements for an existing system.

The County's Waterfall Methodology and Gate Review Approach


PLAN
BUILD
OPERATE
County
Submit Work Request
Approve BE
Approve PMP
Approve UAT Results
Approve Project Closure Agreement
ITPMO
GATE 1
GATE 2
GATE 3
GATE 4
GATE 5
GATE 6
Project Initiation Review
Requirements Review
PMP/Solution Design Review
SIT Readiness Review
UAT Readiness Review
Production Readiness Review
Project Team
PHASE 1 Initiate the Project
PHASE 2 Develop Requirements
PHASE 3 Complete Plans and Solution Design
PHASE 4 Develop Products and Prepare for SIT
PHASE 5 Perform SIT and Prepare for UAT
PHASE 6 Perform UAT and Prepare for Production
PROJECT CLOSEOUT
086 CA CoSD

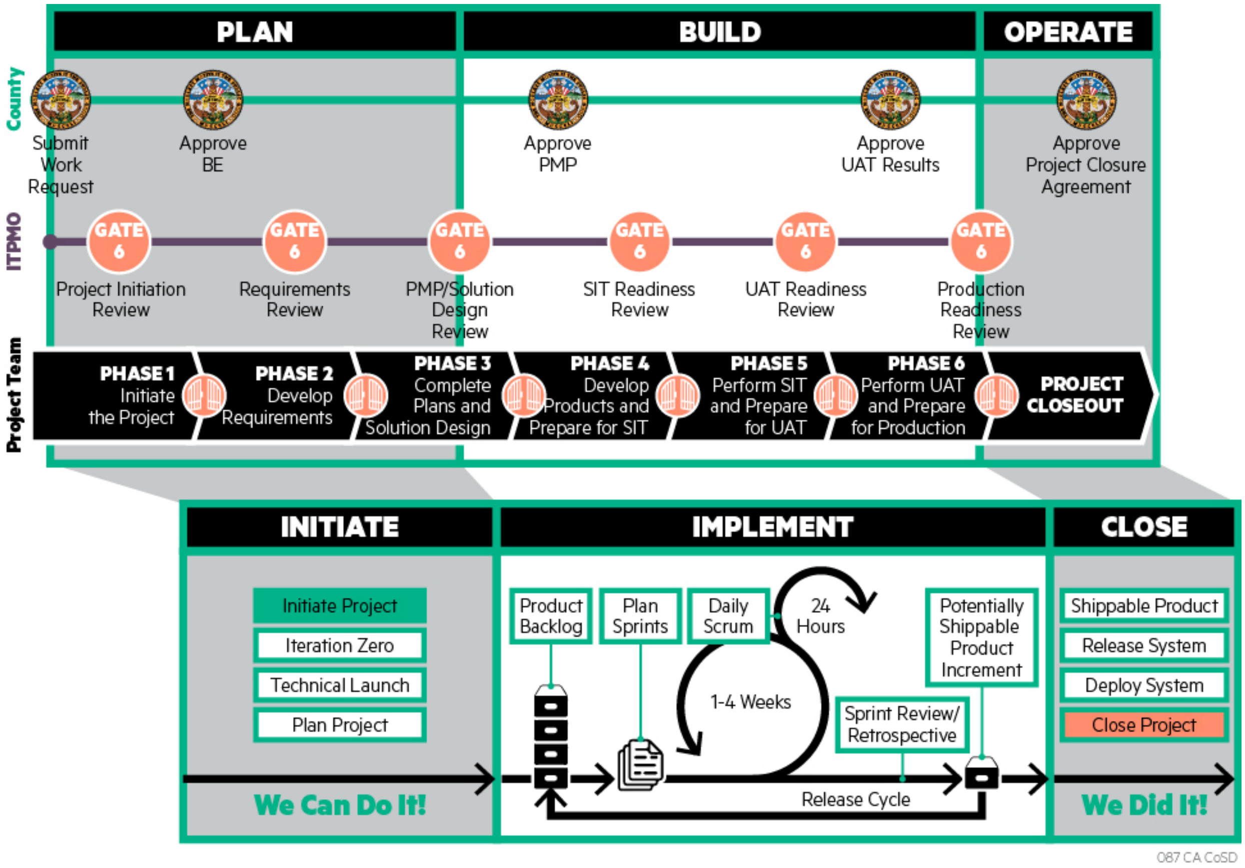
Agile Approach

Contractor tailors an Agile development approach for each project. Based on the Scrum framework, this approach uses an appropriate selection of sound engineering practices from Extreme Programming (XP). It provides a substantial benefit by enabling rapid scalability if required, taking advantage of teams working concurrently in multiple locations, while preserving the ability of rapid response to change.

Scrum Framework

Contractor shall use Scrum Framework process for projects that require a Scrum approach to deliver business applications or to implement major application enhancements for an existing system.

Using County Waterfall Gate Reviews with Contractor Agile Development Process



Contractor maintains County procedures during Contractor's Agile/Scrum development.

- Automated Tools – Automated systems and tools involved in solution

Contractor shall use tools such as HPE's ALM and Dell Marketing's Toad for Oracle software. Contractor shall evaluate other tools that can be used to automate application development services activities and make appropriate recommendations. Contractor shall evaluate automation in configuration and release management as well as the use of HPE cloud service automation and HPE Codar to bring in automation for release management and to integrate with server builds to implement DevOps capabilities.

Contractor's applications development team shall use Contractor Project and Portfolio Management (HPE PPM) demand management module to centralize the resource assignment process. This allows Contractor to strategically manage Contractor's workforce to meet the County's demand across the enterprise. Contractor shall use PPM to track actual effort against project work, allowing quick access to level of effort information that shall be used to inform decisions and prioritize work across all county projects. PPM also has a powerful workflow process engine that helps automate business processes.

8. TRANSITION SERVICES

8.1 Transition Services

Schedule 2.1

Executive Overview

Contractor shall use Contractor's transition and transformation methodology (TTM) as the basis for managing the overall transition as well as the transition projects. TTM shall provide a comprehensive yet flexible, ITIL-aligned framework so that every aspect of the transition is accounted for, planned for, and expertly managed. The Transition Services Management Office (TSMO) shall have primary responsibility for planning and executing the Transition Plan. Contractor shall define and identify key linkage points in the County of San Diego organization. Contractor shall assign a senior and experienced Transition Services Manager (TSM), who shall direct and lead all aspects of the Transition and shall work collaboratively and transparently with the County assigned TSM and Contractor's existing Program Management Office (PMO). The TSM shall facilitate daily stand-up calls and issue weekly status reports to provide transparency and make sure that key decision-makers and the County stakeholders are fully aware of progress as the transition program proceeds.

The TSM shall lead a clearly defined TPMO, with full accountability for execution. The TSM shall report directly to Contractor's Account Executive. In partnership, they shall execute on-going operations and the transition projects.

Requirements

- Description of solution to meet the requirements

Solution Summary

8.1.1 Communications/Governance Plan for the County and the Legacy Provider

Contractor shall provide a Communications and Governance Plan as part of the Transition Initiation activities.

8.1.2 Contingency Planning/Risk Mitigation

Contractor's Transition and Transformation Methodology (TTM) shall include a robust process for Risk Management that shall make sure risks are mitigated to the County's satisfaction.

8.1.3 Measurable Success Criteria

Each project shall, at its inception, include a step where Contractor and the County mutually agree on the definition and measurement of success. This shall provide a smooth cutover process as each framework and project is completed. Success criteria are of two types:

– Project management success criteria:
    - o Signoff of tasks and deliverables according to the dates in the project plan. This shall be measured and reported weekly according to task completion.
– Project deliverable success criteria:
    - o Verification that the business objectives set out for the project were met.

The Transition Services Manager shall be responsible for defining the overall success criteria for the program and submitting it to the County for approval, which approval shall not be unreasonably withheld.

Upon such approval, each Transition Project Manager shall be responsible for managing to and measuring the success criteria for each project under his/her purview. Measurements and tracking against defined criteria for each project shall be reported to the joint Transition Services Management Office (TSMO) weekly. Any measurements that indicate that one or more success criteria are in jeopardy shall be escalated to Contractor leadership for remediation.

Measurement of success criteria may be discrete (pass/fail: either the criterion was met or it was not) or continuous (measurable on a scale, such as a range of percentages). Since project deliverable success criteria is relevant to the County, following are some examples of project deliverable success criteria suggested for this program, along with their measurement approach. This is not intended to be an exhaustive list: as previously noted, actual success criteria shall be established for each aspect of the Transition.

PROJECT	DEFINITION OF SUCCESS	MEASUREMENT APPROACH
Overall Transition Program	Sustainment or improvement in customer satisfaction	• Service Level Measurement, before, during, and after the Transition • Periodic customer surveys, specific to the Transition experience and effectiveness of communications
Disaster Recovery Plan	Completion of one table-top or actual failure exercise according to the new plan	Record levels of participation, scope, and end results and remediation recommendations
Data Center Consolidation	Sustainment or improvement in application performance	Verification by stakeholders that an application migrated to the consolidated data center environment performs as well as or better than it did in its previous environment (as measured by batch job execution times or transaction response times; measurements shall be taken and compared against established baselines conducted and documented prior to Transition, using existing tools such as Autosys or Load Runner or using system based monitors such as performance manager
Email Migration	95% of mailboxes migrated in the first pass without subsequent issues, post-pilot; all remaining issues resolved within 24 hours.	Project team migration results report
Storage Architecture	Zero data loss	Verification from migration tools of successful completion

PROJECT	**DEFINITION OF SUCCESS**	**MEASUREMENT APPROACH**
Development/Test Environment	Successfully implemented Broker and Managed Private Cloud, with all assets assigned to the correct pools	Audit of assets before and after project to verify assignment
Service Portal	80% of End-Users trained on Portal features	Measurement of End-User participation in training

8.2 Transition Project Plan

During Transition Initiation, Contractor shall work with the County to develop the lower-level details of the project plan.

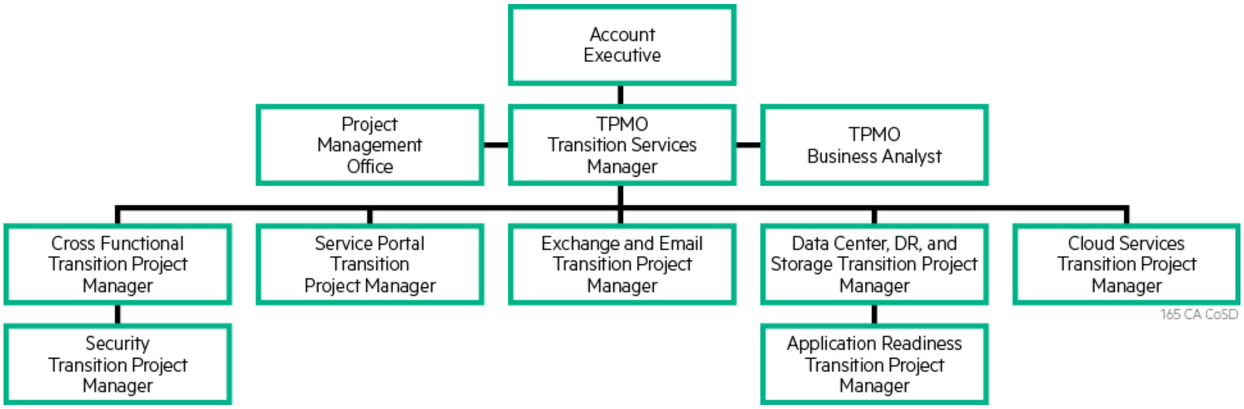
The plan information for each framework can be found as follows:

FRAMEWORK	**TRANSITION PLAN**
Service Desk	• Cross Functional Transition Schedule and Tasks
Application Services	• Cross Functional Transition Schedule and Tasks Special Cross Functional Projects – Application Services Framework,
End User Services	• Cross Functional Transition Schedule and Tasks
Network Services	• Cross Functional Transition Schedule and Tasks
Data Center Services	• Cross Functional Transition Schedule and Tasks • Special Cross Functional Projects – Data Center Services Framework, • E-Mail Services • Development and Test Environment • Consolidated and Single Data Center • Storage Architecture
Cross Functional Services	• Cross Functional Framework Transition: Activities Aligned to Framework Components • Special Cross Functional Projects

8.3 Transition Staffing

The figure below shows the TSMO structure and the roles, functions, and key responsibilities of each member.

Transition Services Management Office


Account Executive
Project Management Office
TPMO Transition Services Manager
TPMO Business Analyst
Cross Functional Transition Project Manager
Service Portal Transition Project Manager
Exchange and Email Transition Project Manager
Data Center, DR, and Storage Transition Project Manager
Cloud Services Transition Project Manager
Security Transition Project Manager
Application Readiness Transition Project Manager
165 CA CoSD

Dedicated Transition Project Managers shall drive each project's success while managing to the integrated plan.

The TSMO shall create and refine joint program schedules, manage risks, resolve issues, provide proper communication, assess progress, and facilitate on-time transition completion. The TSMO shall serve as a central conduit for information, communication, and cooperation. In addition, the TSMO shall manage all project reporting and quality assurance activities to verify that Contractor follows all established Project Management standards and that project reporting is consistent.

Additional details on roles and responsibilities for the identified TSMO staff are presented in the following table. Each Transition Project Manager shall be responsible for the following items:

- Establishing and documenting progress on their individual sub-project plan(s) within the overall master schedule, and coordinating interdependencies with other projects
- Managing the activities of the technical teams working on their projects, in coordination with the current Contractor support staff and within the established operational delivery processes
- Reporting project status to the TSMO with the Project and Portfolio Management (PPM) tool
- Managing issues and mitigating risks that arise, with escalation when appropriate
- Making sure that their project team meets established success criteria and facilitating handoff of the project's deliverables to operations leadership
- Performing close-down of the program.

The role of each TSMO team member is briefly described in the table below.

TSMO Roles and Responsibilities

TMO ROLES	TRANSITION RESPONSIBILITIES
Transition Services Manager	The Transition Services Manager oversees the Transition results, deliverables, schedules, and dependency tracking across all Transition projects. He is responsible for all Transition activities, including Transition kickoff sessions, program and project management, risk management, communication, reporting, Transition escalations, change management, quality management, operational readiness reviews, and coordination with any in-flight projects. The Transition Services Manager performs quality checks during Transition, working with the Contractor account team to make certain that the team conducts all activities in accordance with established practices.

TMO ROLES	TRANSITION RESPONSIBILITIES
Service Portal Transition Project Manager	Responsible for the project to implement and customize the Service Portal, within the Service Desk Framework.
Data Center Consolidation Project Manager	Responsible for the Data Center Consolidation Transition project within the Data Center Framework. This shall include the following projects: • Buildout and migration to the new Data Center Network compartment in Tulsa, and establishment of connectivity to the disaster recovery (DR) site (Contractor-defined sub-project). • Buildout of the new Storage Architecture. • Establishment of the new DR infrastructure to support subscription services in the Colorado Springs HPE Continuity Center. • Execution of the consolidation of all County Data Center workloads currently residing in Plano into the Tulsa Data Center.
Cloud Services Transition Project Manager	Responsible for setting up and configuring the Managed Private Cloud (MPC) and the Helion Managed Cloud Broker (HMCB) in the Tulsa Data Center and configuring the Development and Test Environment within the Data Center Framework.
Application Readiness Transition Project Manager	Works with the Data Center Consolidation Transition Project Manager to coordinate application migration schedules, plans and testing.
Exchange/Email Transition Project Manager	Responsible for migrating the County to the Office 365 email solution within the Data Center Transition Framework
Cross Functional Project Manager	Responsible for the following projects within the Cross-Functional Framework: • Oversight of the delivery of new Standards and Procedures, Service Level Management and Reporting artifacts (or updating current versions to meet the Agreement requirements) for all Cross-Functional Framework Components, as well as for the other Frameworks • Management of development and implementation of the Cross-Functional Framework Component Management Plans • Coordination of delivery of Disaster Recovery Plans for each Framework.
Security Transition Project Manager	As part of the Cross-Functional Framework, the Security TPM shall be responsible for coordinating execution of Security and Identity Management related projects and changes within the other Frameworks.
TSMO Business Analyst	Responsible for administrative support, such as coordinating status reports and meetings, project schedule change management and integration, and quality management on project deliverables.

Contractor's Transition Management Office shall be staffed and ready to begin as of the Contract Effective Date.

During the Transition period, Contractor shall augment Contractor's technical staff with additional resources to make sure the Transition projects execute successfully, without creating undue constraints on the current support teams. Where appropriate, Contractor may temporarily backfill select members of the local team supporting the County so that they may lend their expertise and County knowledge to the implementation of some Transition projects. Contractor shall make sure, however, that this does not cause any disruption to the County’s current services and projects.

Rationale

Contractor shall manage each sub-project as a project, while continuing to provide excellent service delivery. During the Transition period, Contractor shall successfully plan, communicate, and manage the transition activities collaboratively.

- Deployment plan for resources and use of facilities

Resources. Contractor shall provide dedicated resources for Transition project management and execution to make sure that operational delivery and the County’s in-flight projects are not impacted by resource constraints.

Facility. The Contractor Transition teams shall support the Transition from Contractor’s Rancho Bernardo site and existing County locations, where appropriate, as well as Contractor’s facilities in Tulsa, OK, and Colorado Springs, CO. TSMO resources, including the Transition Services Manager, shall operate out of the Rancho Bernardo site.

- Key methodologies and processes in solution

Contractor shall execute project management, transition, and transformation by using Contractor’s Transition and Transformation Methodology (TTM) composed of standardized processes, methods, tools, and governance to deliver repeatable and predictable results. It shall address the people, business processes, and technology issues of transition and provides a step-by-step process for joint planning, communication, post-contract verification, and management.

Contractor TTM Process

Contractor shall use Contractor’s comprehensive and proven TTM, a flexible comprehensive framework of robust processes, procedures, best practices and supporting assets that enable the successful planning and execution of a Transition or Transformation program. It shall define what deliverables are to be produced, what work needs to be done, who should do it, how they should do it, and when it needs to be done. It shall also provide supporting assets to complete the work efficiently.

Transition programs and their associated projects shall go through five distinct phases: Initiate, Plan, Execute, Monitor and Control, and Close.

Initiate. Contractor and the County shall set up the program management structure described above, onboard the program team, and start the program. During the first few days of the Transition, Contractor’s TSMO shall create draft versions of the Communication Plan, Governance Plan, and the initial master Transition Project Plan and Schedule. Contractor shall start from Contractor’s template repository and work with the County collaboratively on these items, but shall also submit a final draft for formal County approval as required. Once finalized and approved, Contractor shall put these plans into action and begin program execution.

Plan. Building on the notional Transition Plan developed during the proposal process, Contractor shall conduct detailed joint planning to elaborate and refine the plan, then conduct a transition kickoff meeting with identified key stakeholders from the County, the current delivery leadership—as represented by Contractor’s key personnel—and key leaders from the Transition Technical teams.

The TSMO shall create a master Transition Management Plan along with a corresponding Transition Schedule. This shall serve as the overall foundation for the program and shall address the key program elements, including resources, dependencies, and timeframes. This master plan and schedule shall be augmented for each of the six Transition projects. The figure below provides a high-level timeline of Transition activities, showing the Transition Initiation, the Framework Transitions, and the Final Transition Milestones that follow at the end of the Transition period.

Execute. Within the TTM methodology, each Transition Project Plan shall be executed as described in the sections that follow.

Monitor and Control. Throughout the program, the TSMO shall oversee the Transition activities to produce deliverables on time, remain within budget, and execute Change Management if needed.

Close (Final Transition Milestones). Contractor shall ensure that commitments and success criteria defined in the Transition Management Plan have been met.

- Automated systems and tools involved in solution

The following table lists the tools Contractor shall use to support the Transition program.

Tools Utilized to Support Transition

TOOL NAME AND VENDOR	DESCRIPTION
TTM Templates	• Integrated Transition and Transformation Plan (ITTP) • Transition Specific Risk Register (Excel) • Communication Plan (Word) • Governance Plan (Word) • Transition Daily, Weekly Meeting minutes (Word) • Operational Readiness Checklist / Success Criteria (Word)
Project-specific Tools	• Contractor shall use Microsoft Project to coordinate and manage Transition-related projects and tasks. • Tools used for Transition projects shall be defined and covered in the related sections.

8.3.1. Transition Management Specific Questions

Transitioning licenses, contracts and leases from the Legacy Provider and the County

Contractor shall support and manage all third-party vendor relationships, licenses, contracts, and leases.

Contractor shall create and submit for County approval a process to transfer licenses, contracts, and/or leases, that are included within a Service provided under the Agreement.

Transition resources that shall remain to provide Operational Services for the County versus resources who shall transfer after Transition

Contractor shall provide dedicated resources for each transition project. Contractor shall leverage Contractor resources supporting the County and Contractor's staffing plan shall include subject matter experts (SME) to augment and make sure that there are no impacts to operations activities.

Cross Functional Services

- Description of solution to meet the requirements

Solution Summary

Contractor shall implement Security and Identity Management changes required to meet each framework's delivery model, in those cases where changes are required. The cross functional activities for each framework shall be implemented in parallel but in coordination with that Framework's Transition projects, where applicable. For frameworks that do not have specific transition projects identified, the Cross Functional Transition shall be the only scope of that framework's transition.

During the Transition period, Contractor shall develop a management plan for each of the Cross Functional component areas and train Contractor's teams on the changes. For the Cross Functional components, Contractor shall update the Standards and Procedures Manual, Service Level Management, and Reporting during the 270 days of the Transition period, so these efforts shall follow a similar approach to that of the other frameworks.

- Deployment plan for resources and use of facilities

The Cross Functional Transition activities shall require input and participation from Contractor support staff to make certain that processes and deliverables leverage existing artifacts and methods. The Cross Functional Transition team shall be embedded with each Framework Transition team.

Contractor shall support the Cross Functional Transition primarily from Contractor's Rancho Bernardo site.

- Key methodologies and processes in solution

Transition Schedule and Tasks

The chart below is a high-level example of the Cross Functional activities within a Service Framework: End User Services. The same task structure shall apply to each framework as well as each Cross Functional component.

While the task structure shall be the same across frameworks, task durations shall vary based on the degree of change being introduced by the Agreement requirements.

Although many activities shall happen in parallel, once Contractor creates the schedule for all Cross Functional components and the Cross Functional activities for each framework, the timeline shall expand with the details and dependencies.

The figure below shows the core high-level tasks Contractor shall perform for each framework.

There are no dependencies identified for generation of the Cross Functional Component Management Plans, which shall be developed in parallel with, and as the culmination of, the other component artifacts.

Cross Functional Activities Aligned to Service Frameworks

Within each Service Framework, Contractor shall follow the basic task structure illustrated in the figure below.

Standards and Procedures. Contractor shall inventory and review each procedure document against the Agreement to identify the subset of processes that need to be changed or created (if a new process is needed). Contractor shall then categorize the documents based on the degree of changed required:

- Completely new procedure or standard needed – If a new process is being implemented in support of a new technology, Contractor's Solution Guide documentation for the service offering that Contractor is implementing shall provide a base set of procedure documents. From there, Contractor shall customize and adapt those base documents to the specifics of the County's environment and documentation standards. Contractor shall then test the procedure and further refine the documentation. If a new procedure is needed based on a new business requirement, Contractor can use Contractor's Enabling Delivery and Global Excellence (EDGE) repository to locate a base artifact from which to build the new procedure.
- Updates required to an existing procedure – Contractor shall follow a similar process to the one for a new procedure/standard, but the starting document shall be the existing process. Whether testing is required shall depend on the degree of change.
- Existing procedure continues unchanged – No modifications required.

Once the Standards and Procedures drafts are complete, Contractor shall submit each draft to the County for review and response. The County shall reply within the agreed timeframe if any changes or clarifications are required. Contractor shall then make the final set of modifications, if needed, and finalize the documentation. Documents shall be posted to the appropriate repository reachable from the Service Portal. Any procedures or standards that are no longer valid shall be retired and their documentation archived according to Contractor's Records Management policy.

Where appropriate, Contractor shall provide training in and/or communications about new or modified procedures and standards to Contractor's staff and to County stakeholders who participate in or are customers of the process. Training methods shall range from Frequently Asked Questions (FAQs) and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training at Contractor's Rancho Bernardo site.

Service Level Management. During the Cross Functional Transition, Contractor shall adhere to the following steps to implement Service Levels:

For each new or modified Service Level, Contractor shall identify the data necessary to calculate it, the process to verify data quality and scrub exceptions, and any scripting or automation needed to manage the data and its reporting to the Service Level Management process.

Contractor then shall develop and test the new or updated metrics collection process, checking the data and the performance metrics.

Contractor shall identify the appropriate process or service improvements needed to meet the Service Level and test them for an additional month to determine whether this brings Contractor to an acceptable level of performance. Generally, no more than one to three iterations of baseline measurement and adjustment are required to identify the scope of operational change required by the Service Level. The time to complete this process shall be within the time allocated for transition of the applicable framework.

Once Contractor has successfully achieved the new performance target, Contractor shall proceed to update all process and reporting artifacts, and present them for County review and response, according to the steps described above in Standards and Procedures. After finalization, Contractor shall post all deliverables to the appropriate repository, available from the Service Portal.

Once implemented, Contractor's Service Level metrics shall be integrated into the Service Level Dashboard), available from the Service Portal.

Reports/Deliverables. Transition activities for creating new or modified reports shall be similar to the tasks defined for updating Standards and Procedures: Contractor shall inventory and review each report against the Agreement to identify the subset of reports that need to be changed or created. Contractor shall then categorize them based on the degree of changed required:

- New report needed – If a new report is being implemented in support of a new service, Contractor shall create or customize and adapt existing deliverables, or the automated scripts that create them, to the specifics of the County's environment and reporting standards. Contractor shall then test the report and further refine the process. If a new deliverable is needed based on a new business requirement, Contractor can use Contractor's EDGE repository to locate a base artifact from which to design and automate the new report.
- Updates required to an existing report – Contractor shall follow a similar process to the above, but the starting point shall be the existing report process.
- Existing report continues unchanged – No modifications required.

Once drafts of the new or modified reports for the framework are ready, Contractor shall submit them to the County for review and response. The County shall reply within the agreed timeframe if any changes are required. Contractor shall then make the final set of modifications, if needed, and finalize the generation procedures and formats, and place the reports into an automated schedule wherever possible. Process documentation shall be posted to the appropriate repository, as described above, and new reports shall be added to the standard reporting cycle.

Where appropriate, Contractor shall provide training in and/or communications about new or modified procedures and standards to Contractor's staff and to County stakeholders who participate in or are customers of the process. Training methods shall range from FAQs and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training in Contractor's Rancho Bernardo site.

Security and Identity Management Updates. In general, transition tasks shall follow the steps illustrated in the Gantt chart, but for security sub-projects, Contractor shall add more detail shall to address specific requirements.

Framework Disaster Recovery Plan. Contractor shall add disaster recovery (DR) specialists to augment the team. They shall be dedicated to maintaining these plans and overseeing DR testing. They shall join the Cross Functional team during transition to lead the DR plan updates for each framework. Each framework shall have its DR plan reviewed and updated to support the requirements of the Agreement. The DR plan shall be submitted in draft form for County review and comment, then finalized and delivered to a restricted area of the Service Portal no later than 90 days prior to the framework cutover[1].

Special Cross Functional Projects – Service Desk Framework

No special Cross Functional projects have been identified for the Service Desk Framework. The project to implement the Service Portal is described in the section for Service Portal transition.

Special Cross Functional Projects – Application Services Framework

Two special Cross Functional projects have been identified for the Application Services Framework that are illustrated in the table below.

Special Service Levels: Application Availability and Application Response Time. The process to implement these two Service Levels shall be similar to that described above.

SaaS Application Onboarding: The County has identified in the solicitation 169 applications identified as SaaS applications that Contractor does not currently support. For each of these that the County wishes Contractor to support, Contractor shall need to perform the steps described in the Gantt chart below.

Contractor shall review each application that the County wants Contractor to support, according to Contractor's established process for Third Party Agreements, and determine the level of support possible for each (license transfer, right to use, warm transfer). Once Contractor has a final list, Contractor shall work with the support contacts at that vendor to understand their support process, and create Service Desk scripts that shall enable Contractor's team to field those calls. Contractor shall then train Contractor's Service Desk staff to support them, and prepare communication materials for users of those applications to understand the new support process.

All draft materials shall be submitted to the County for review and comment. The County shall reply with any changes required within the agreed timeframe, after which Contractor shall finalize and post all deliverables to the Service Portal and cut over support for those applications during the Application Services Transition.

Special Cross Functional Projects – End User Services Framework

No special Cross Functional projects have been identified for the End User Services Framework.

Special Cross Functional Projects – Network Services Framework

No special Cross Functional projects have been identified for the Network Services Framework. The re-architecture and refresh of the Tulsa Data Center network is described in the Data Center Consolidation Project.

Special Cross Functional Projects – Data Center Services Framework

A number of security projects have been identified for the Data Center Services Framework. These include the following:

- Projects to re-orient services that are active-active across sites in the two-data-center model, such as Active Directory, Active Directory Federation Services (ADFS), and the Endpoint Threat Protection core.
- Projects in support of the email transition to cloud, such as adaptation of the Security Incident Management process.
- Projects to address heightened security requirements, such as expansion of security information and event management (SIEM) services, design and implementation of a separate Development/Test network zone, and implementation of continuous scanning.
- As part of the Data Center network buildout, Contractor shall convert from Checkpoint firewalls with TippingPoint for intrusion detection/prevention services to Palo Alto devices that support both functions.

Special Cross Functional Projects – Replacement of myRequests

During the Cross Functional Transition, Contractor shall replace the myRequests Service Request system with the Service Catalog and Request Manager that comes pre-integrated with HPE Service Manager. Because this migration takes longer than the Service Portal implementation, during the initial deployment of the Service Portal, the Service Portal shall be linked (using a front page tile or from the "Links" tile, at the County's discretion) to the myRequests system, and Contractor shall maintain myRequests following Contractor's processes, while the new request manager/service catalog functionality is being configured. Once the new Request Manager system is ready, and End-User training has taken place, Contractor shall disengage the link to myRequests and bring Request Manager online.

Special Cross Functional Projects – Identity and Access Management (IAM)

Contractor shall provide the following Identity and Access Management implementation services as part of Transition, with ongoing support included in the IAM RU:

- Initial IAM plan for County approval
- Identity Provider capability (Oracle Federation Manager) for the initial use case up (i.e. DCSS) for a maximum of five (5) applications
- Attestation functionality for County review of End-User access. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part and the On-Boarding of the first five (5) applications utilizing provisioning via automated workflow process.
- Capability for County to track and maintain End User access privileges for County users. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part 1 project as well as the implementation of attestation functionality.
- Monthly reporting on changes to the IAM repository. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part 1 project and the onboarding of the first five (5) applications utilizing provisioning via automated workflow process.
- Institute an architecture principle in the design phase of new applications that designates IAM as the single solution for County identities and the use of the enterprise sign on function
- "2.18.2.5 IAM Workflow Automation" project for the amount of $1,633,874.113 consists of two parts as follows:
    - "CSRF Replacement Workflow Automation" – Contractor shall complete the Workflow Automation project and associated requirements for a firm fixed price of $1,228,874. High level descriptions are below:
        - An automated workflow to assign access management requests. The automated workflow process shall create the appropriate line items for the access management teams to manually provision the IDs. Note: this extends past transition since data population is dependent on the completion of Phase I (County funded project) of On-Boarding The Computer Service Requests Form (CSRF) shall be retained for future review and reporting functions as an audit trail.
        - Onboarding up to five (5) applications, at County sole discretion, to utilize provisioning via the automated workflow process, after project completion. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part and the On-Boarding. Candidate applications must be only provisioned via Active Directory group membership.
    - "PeopleSoft On-boarding Phase II" – County shall fund and Contractor shall complete the PeopleSoft On-boarding Phase II project for a work effort up to and not to exceed

$405,000. Contractor shall make all reasonable efforts to complete the project within the $405,000 to the best of the Contractor ability. Any work effort exceeding $405,000 shall require a County-approved Change Request to be funded by the County. This project is dependent on the completion of the PeopleSoft On-boarding phase I, which is in progress, and it is County funded under County Work Request SD-WR-024804. PeopleSoft On-boarding Phase I is intended to be completed June 2017.

Cross Functional Framework Transition: Activities Aligned to Framework Components

For the Cross Functional Framework components, the Transition shall follow the same basic structure as described above for the frameworks. The table below summarizes the approximate scope of change in each Cross Functional component. The extent of change to each component has been categorized as follows:

- Limited – changes are expected to be minor updates to existing processes and deliverables
- Medium – some new processes or deliverables—generally similar to current practices
- Large – multiple new processes or deliverables—Organizational Change Management applies

Approximate Scope of Change for each Cross Functional Component

FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Contract and Acquisition Management Services	Minimal	None
Integrated Asset Management Services	Limited	Contractor shall integrate data from AT&T Asset Management Systems
Billing Management Services	Limited	Setup of billing processes for new Resource Units
Security Management Services	Large	Multiple Security sub-projects within the Data Center and Network Frameworks, as described above.
Service Delivery Management Services	Medium	New component
Project Management Services	Limited	None
Integration and Testing Services	Medium	New component
Incident Management Services	Limited	New component
Problem Management Services	Limited	New component
Change Management Services	Limited	New component
Release Management Services	Medium	New component
Configuration Management Services	Limited	None
Capacity Planning and Performance	Medium	Metrics collection and reporting from new technologies: Helion Managed Private Cloud (MPC) and Helion Managed Cloud Broker (HMCB)

FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Disaster Recovery Management Services	Large	Implementation of new architectures and addition of Business Continuity specialists to the support team
Identity and Access Management Services	Large	Modification of AD and ADFS architectures to support a single data center model, automation of Access Management Workflows to replace the CSRF form, IDAM transition, and PKI transition.
Reporting Management Services	Large	Implementation of the Service Portal and Data Analytics shall drive significant improvements in this area
Domain Name Management Services	Limited	None
Business Analyst Services	Medium	New Component
Chief Technology Architect	Limited	None
Enterprise Application Architect	Limited	None
Innovation Officer	Limited	None

The basic steps for developing the Cross Functional Component Management Plan shall be the same as those for creating new procedures. Upon County approval, the Cross Functional Component Management Plans shall be published on the Service Portal.

- Automated systems and tools involved in solution

Information feeds from various operational tools shall be used to provide Cross Functional Service deliverables.

No tools beyond those already described for managing the Transition process are required to transition the Cross Functional Framework.

E-Mail Services

- Description of solution to meet the requirements

Solution Summary

Contractor shall move the County to Office 365 Exchange Online.

Contractor shall work with CTO to identify the move groups, determine success criteria and finalize timing. Next, Contractor shall execute a proven HPE methodology, Migration Factory (MF). MF is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft Office 365 Government Community Cloud. Contractor shall move County users in waves from Exchange to the MS Cloud over an 8- to 10-week period.

The email migration described above shall cover non-inbox PSTs that are in the current inbox. Contractor shall, in a separate PST Migration Project, migrate users’ PST files to their Exchange Online Mailbox.

The PST Migration Project shall parallel that of the inbox migration and complete at approximately the same time.

Rationale

The Service Desk shall own tickets from start to finish in support of both Exchange and Office 365 environments.

This migration shall be accomplished prior to the end of the Transition Period, negating the need to upgrade the existing Exchange 2010 environment, allowing the data center based email infrastructure to be retired when the migration is complete.

- Deployment plan for resources and use of facilities

Members of Contractor's U.S. Messaging Practice, in coordination with CTO, shall both plan and execute the migration, with support from the local. A transition project manager shall guide the entire process, and County users shall be supported by the Contractor's Service Desk.

Contractor shall complete the migration virtually and at the Plano and Tulsa data centers. Microsoft engineers shall use the County ticketing system to support trouble tickets during the migration and provide experts to resolve issues if needed.

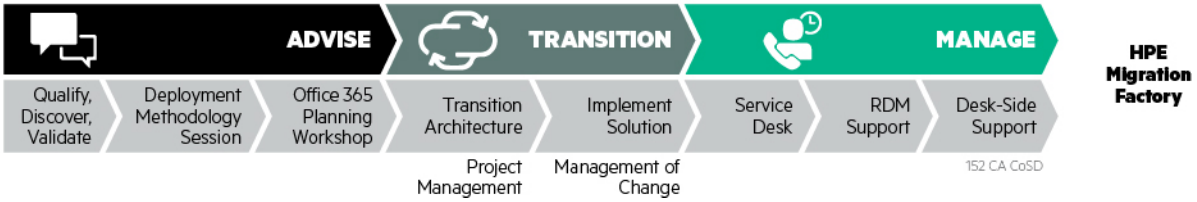
The County's Office 365 environment shall reside in the Microsoft Office 365 Government Community Cloud environment. This a hardened U.S.-based environment that is FedRAMP authorized, and whose support personnel are appropriately screened. It has features that can support Criminal Justice Information Services (CJIS) requirements for law enforcement agencies, and IRS-1075 requirements for customers who handle Federal Taxpayer Information (FTI).

- Key methodologies and processes in solution

Contractor's dedicated E-Mail migration practice shall be built on standard processes, tools, and trained personnel to assess, prepare, implement, and then decommission Exchange.

The Office 365 transformation methodology shall follow Contractor's standard advise, transition, and manage approach that closely follows the County's plan, build, operate formula (see figure below). Messaging engineers shall provide due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel shall use to move from Exchange 2010 to Exchange Online.

Contractor's Advise, Transition and Manage Approach



Transition Schedule and Tasks

Contractor shall provide the final E-Mail Transition Plan and Schedule for County approval.

PST Migration shall follow a similar high-level methodology but with a simpler work breakdown. The basic process for PST Migration shall be as follows:

- PST Discovery: PST files are scattered among file shares and even local disk drives of End-Users. They shall be found via domain-level discovery of End-User shares and drives.
- PST Harvesting: Those files are then gathered in a central file store, linked to the End-User's Exchange Online account, and readied for import.
- PST Transfer: Whereas PSTs can be imported to Exchange Online via transfer over the WAN, for the large number of mailboxes and potentially large data sets, Contractor shall use Microsoft's Import Service via drive shipping. The data sets are stored on an encrypted drive and transported to Microsoft for import. This significantly reduces the amount of time for WAN transport of 15,000+ separate PST files.
- PST Import: Microsoft shall import the users' PSTs to their individual Archive Mailboxes. There is no size limit to the amount of emails that may be stored in Archive Mailboxes.

Plan and Design. For the Email Migration project, during the planning period, Contractor shall create the detailed migration plan and present it to the County for review and approval. As part of this process, the U.S. Messaging Practice, with advisement from the current email support staff, shall assess the environment, size the migration temporary infrastructure needs, and mitigate any potential or actual issues.

Configure. Contractor shall set up temporary infrastructure, configure the migration tool virtual server, configure DNS and network, and deploy a hybrid server. After system integration testing is successfully completed, Contractor shall perform a pilot launch.

Pilot Program. The Migration Factory shall perform a pilot migration on a subset of users defined by CTO, moving them to Office 365 and seeking feedback on their experience. Contractor shall conduct UAT in collaboration with the County, review results, and adjust Contractor's plan as needed based on the results and End-User feedback.

Documentation and Training. Contractor shall prepare service documentation, training materials, and Service Desk scripts to prepare for the migration waves. The County shall review the deliverables, Contractor shall respond to questions or clarifications, and then seek final approval to proceed. The completed documents and training material shall be added to the Service Portal, and Contractor shall train Contractor's Service Desk agents and other support personnel. Contractor shall review with CTO to determine if other types of training may be required and deliver that training accordingly.

Migration Waves. Contractor's Migration Factory shall then begin executing the migration move groups moving each group's mailboxes from the Exchange servers to the Microsoft Office 365 Government Community Cloud. Contractor shall complete the migration during an 8- to12-week period. As groups are migrated in waves, Contractor shall move into the manage phase, providing support.

Project Completion. Contractor shall request final County approval and sign-off. After all users are migrated and County approval is received, the E-Mail migration shall be complete. Similarly, after all PSTs have been migrated to users' archived mailboxes, the PST Migration shall be complete.

- Automated systems and tools involved in solution

To accomplish migration, Contractor shall provide and use Contractor internally developed software and a migration tool from Binary Tree Company. Contractor shall use a utility available from Microsoft for migrating PSTs.

Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
E2E by BinaryTree Corporation	• Analysis and migration engine for migrating on-premise Exchange mailboxes to Exchange Online • Allows rapid, low-risk migrations of large Exchange End-User populations. • This is the preferred tool of Contractor's messaging engineers
PST Capture	• Microsoft tool for searching and harvesting PST files

Development and Test Environment

- Description of solution to meet the requirements

Solution Summary

Contractor's solution for Dev/Test shall be tightly linked to the data center consolidation and the evolution of the Data Center to a hybrid environment: it shall use the Helion Managed Private Cloud (MPC), as described in the Data Center Consolidation Transition Project, and Helion Managed Cloud Broker (HMCB) to provide a business-rule defined boundary for Dev/Test capacity. This allows the environment's composition of server sizes and platforms in the hybrid environment to evolve and change over time in response to changing requirements without exceeding the County's established financial parameters. Contractor shall define thresholds to warn when the environment is approaching those limits.

Contractor shall provide a persistent Dev/Test environment for all P1 and P2 applications, so that high-priority County applications are guaranteed the resources needed to conduct testing in support of production issues (Applications Maintenance and Operations) or development projects. Contractor shall also maintain surplus space in the Dev/Test environment beyond that needed for the P1 and P2 applications to accommodate non-persistent Dev/Test capabilities for P3 through P5 applications. The surplus space shall be used on an as-needed basis to support the normal development and test activities of these lower-priority County applications. Contractor shall control the cost of the overall Dev/Test environment while also providing ample capacity for the County's suite of applications.

Contractor shall manage Dev/Test workloads within a SAN-based repository visible to the private cloud and perform tasks such as boot up and shutdown of virtual machine images on demand. Upon the County's request/approval, tasks shall commence. The Dev/Test environment shall have interfaces enabling connectivity to the Production environment to meet business needs. Contractor shall secure these interfaces with virtual local area networks (VLANs) and access control lists (ACLs). Identity access management services shall be applied across all County environments, including Dev/Test.

Contractor shall implement the HPE Codar toolkit to create an automated Release Management Framework in the Dev/Test environment. This shall support the evolution of Contractor's Applications Development Services to adoption of DevOps practices.

Rationale

Transition to MPC and HMCB shall provide an integrated platform for Dev/Test services that mimics the Production environment to streamline application development and deployment. HMCB shall provide the tools to create the hybrid design that the County is looking for in this environment. These tools provide the flexibility to include or exclude any type of platform within the Dev/Test scope, and manage its size based on a financial and business viewpoint instead of having to be concerned about the exact mix of hardware and software. Contractor can make this definition all-inclusive or create the business rules to be less flexible according to the County’s preference, without impacting the project timeline or plan. As the County’s environment becomes more standardized, Contractor can collaborate to adjust the Dev/Test environment parameters to suit evolving requirements without reconfiguring the underlying technologies.

Because these tools are used to support applications in both Dev/Test and Production and are a key component of the Data Center Services Framework, transition of Dev/Test is designed to occur in conjunction with the remainder of the framework.

- Deployment plan for resources and use of facilities

The Data Center Consolidation Transition Project Manager (TPM) shall be directly responsible for activities associated transition of the Dev/Test environment. The Data Center Consolidation TPM shall be supported by the Cloud Services TPM, responsible for the MPC and HMCB services portion of the Transition. Contractor’s virtual support team shall include architects, engineers, and migration specialists with expertise in cloud services and experience building out these environments for other clients.

The existing data center facilities in Tulsa and Plano shall support transition of Dev/Test until migration of all workloads is complete.

- Key methodologies and processes in solution

Transition Schedule and Tasks

Those tasks unique to the Dev/Test environment begin where Contractor configures the HMCB to establish virtual boundaries for the Dev/Test environment and other resource pools as needed. The preceding tasks are shown for context.

Planning and Build Phases. During the Consolidation Assessment task, Contractor shall build a migration roadmap detailing the placement, plan, design, and execution of migrations of development and testing workloads residing in Tulsa and Plano.

Once the hybrid architecture is built out, the Contractor’s engineering and applications team shall collaborate with the County to define and size the composition of the Dev/Test portion of the environment, defining the financial parameters for each type of environment to be included. Dev/Test traditional servers already resident in Tulsa shall be included immediately; as servers from Plano migrate into the environment, they shall be imported into HMCB.

HPE Codar Environment Tasks. Once the Dev/Test environment is defined and built, Contractor shall design the environment for automated release management. This shall include design and configuration of the infrastructure, implementation of the software tools and necessary processes to manage them, and testing with a sample application.

Migration to Dev/Test. Contractor's migration engineers shall coordinate closely with the Application Development team to be aware of in-flight projects and migrate these at the proper time, in a non-disruptive manner.

Contractor shall prioritize move groups, with Plano workloads coming into Tulsa having the highest priority. This shall allow the County to consolidate into Tulsa as quickly as possible, to meet consolidation objectives. Contractor shall migrate all remaining non-production workloads into the Dev/Test environment (either by actual migration into the MPC or by including them in the virtual boundary created by the HMCB).

- Automated systems and tools involved in solution

Contractor shall use the same automated tools as described for, Consolidated and Single Data Center.

Consolidated and Single Data Center

- Description of solution to meet the requirements

Solution Summary

With the consolidation, Tulsa shall become the single production data center, and Contractor shall migrate all services from Plano to Tulsa. Contractor shall build a DR environment for the County at the Contractor's DR site in Colorado Springs, CO. It shall provide failover capability for applications that require DR, core services, and data center security services.

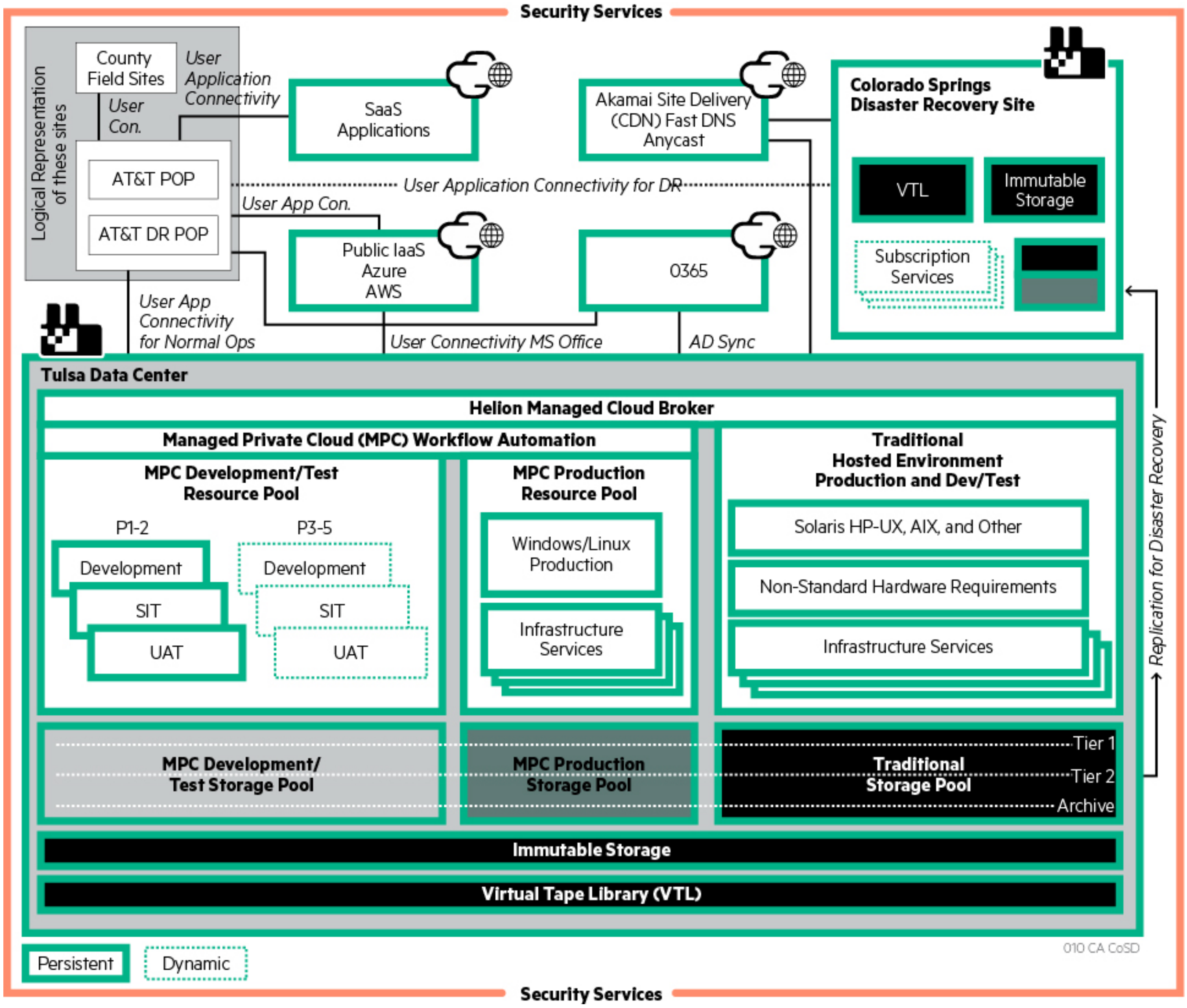
Contractor's structured transition approach for the data center consolidation shall be comprised of the following subprojects. These shall be completed in the sequence listed below to accomplish a smooth and non-disruptive transition.

- Set up and configure the data center network and security infrastructure to meet the new requirements.
- Refresh the data center storage environment to meet the requirements
- Build out the hybrid management capability and prepare the Tulsa data center to receive the server capacity currently resident in Plano. These activities shall be performed in parallel with the instantiation of the DR capability, and shall include the subproject to set up the development and test (Dev/Test) environment.
- Migrate applications, and in some cases, equipment, from Plano to Tulsa, based on a move group schedule provided by Contractor and upon approval by the County.
- Migrate the County's mail presence from the current Exchange environment to the Microsoft Azure Government instance of Office 365. Note that this project is not dependent on the ones above—it can be executed before or in parallel with them—but must be completed before the Plano environment can be decommissioned.

For each component identified above, Contractor shall provide a specific transition plan, interlocked with its related plan and the master schedule that details the tasks, milestones and schedule, for approval by the County. Throughout the project, Contractor shall work collaboratively with the County to develop success criteria, validate the scope and deliverables, and provide regular communication of the project's status, anticipated risks or issues, and Contractor's mitigation approach to make sure potential problems do not interfere with project completion.

The figures below provide an overview of the consolidated data center post-transition and briefly describe each component of the consolidated data center associated with the transition.

Consolidated Data Center Overview

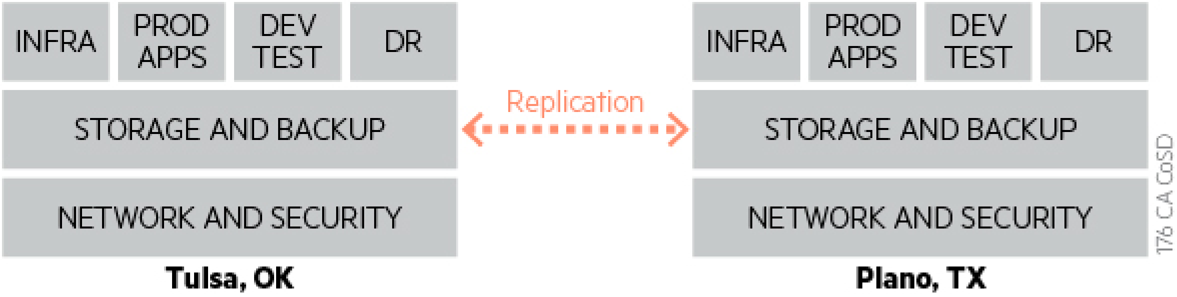

Security Services
Logical Representation of these sites
County Field Sites
User Con.
User Application Connectivity
AT&T POP
AT&T DR POP
SaaS Applications
Akamai Site Delivery (CDN) Fast DNS Anycast
Colorado Springs Disaster Recovery Site
VTL
Immutable Storage
Subscription Services
User Application Connectivity for DR
User App Con.
Public IaaS Azure AWS
0365
User App Connectivity for Normal Ops
User Connectivity MS Office
AD Sync
Tulsa Data Center
Helion Managed Cloud Broker
Managed Private Cloud (MPC) Workflow Automation
MPC Development/Test Resource Pool
P1-2
P3-5
Development
SIT
UAT
Development
SIT
UAT
MPC Production Resource Pool
Windows/Linux Production
Infrastructure Services
Traditional Hosted Environment Production and Dev/Test
Solaris HP-UX, AIX, and Other
Non-Standard Hardware Requirements
Infrastructure Services
Replication for Disaster Recovery
MPC Development/ Test Storage Pool
MPC Production Storage Pool
Traditional Storage Pool
Tier 1
Tier 2
Archive
Immutable Storage
Virtual Tape Library (VTL)
Persistent
Dynamic
010 CA CoSD
Security Services

The Data Center Consolidation shall result in a modern hybrid environment.

Data Center Consolidation – Overview of Steps

The figures that follow describe the high-level steps for the consolidation project. The figure below depicts the County Data Center environment (Plano and Tulsa only), showing the basic classifications of servers and infrastructure as they are in place today.

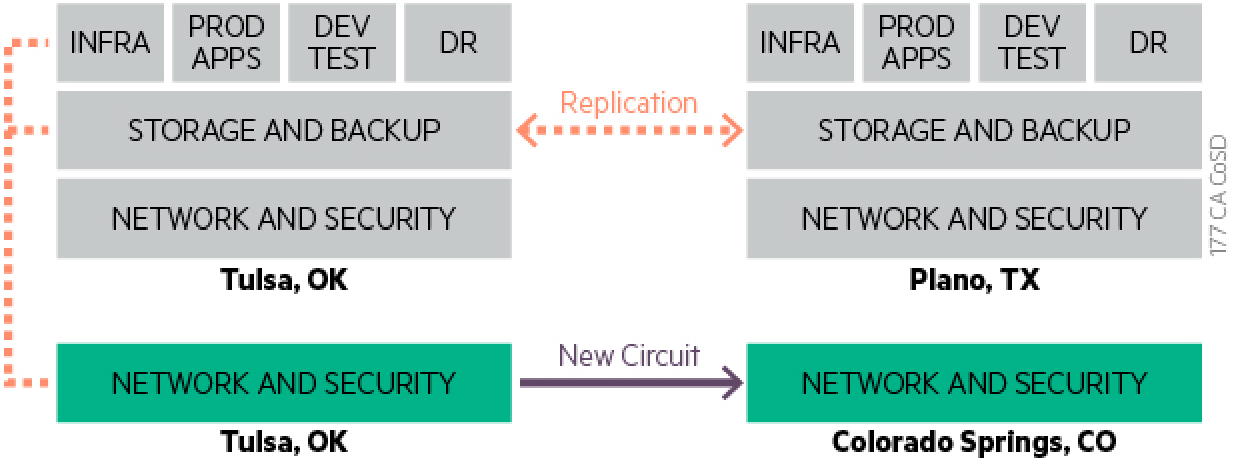
Current Data Center Environment



The first step, shown in the figure below, shall be to build out the new Data Center network compartment with the new network and security components. The new network compartment in Tulsa shall be built out in the same physical room as the current Tulsa environment. Its components are described in the second figure below. In parallel with the Tulsa network buildout, Contractor shall build out the network compartment for the DR environment in Colorado Springs.

The process to refresh/replace the network environment shall follow an "A/B" migration approach. Contractor shall build out the new network infrastructure (e.g., load-balancers, firewalls, switches, routers) reproducing the existing configurations on the new equipment. When Contractor has tested and verified the configurations, it takes a change window to shut down the "A" side of the environment (all traffic seamlessly fails over to the "B" side), and bring up the new equipment's "A" side. Contractor shall reroute the traffic to the new equipment and verify proper operation. Once Contractor is certain that no failback is needed, Contractor shall replace the "B" side of the equipment with the new equipment (again, in a controlled change window), re-test the failover, and once all is operating correctly, remove the old equipment.

New Network Compartments in Tulsa and Colorado Springs



Internet Connection. Leveraged Internet Service (LIS) provides shared Internet connections in a multi-tenant data center. Contractor shall obtain and manage the Internet connectivity to the data-center itself, and then extend that connectivity to applications in the data-center. Each LIS core router shall be connected (using link-aggregation) to both of the two WAN connectivity Layer-Aggregation Switches (WCL-AS) for the data center. Each LIS core router shall also terminate a connection from a separate ISP to provide diverse connections. The WCL-AS connections shall provide the path to the downstream LIS customer environment.

WAN Connectivity. The Contractor's data center shall be connected to the DR site using Ethernet MPLS WAN connectivity to provide high-speed data transmission, connecting back into the County's Points of Presence (POP). Connectivity shall be sized to 250Mbps of bandwidth with the capability to increase up to 1Gbps. Contractor shall have the capability of meeting any annual bandwidth increases should the County require. Within the Contractor's data center, Contractor's support team shall manage the dedicated WAN devices. Within the County POPs, Contractor shall ensure that AT&T manages the dedicated WAN devices. All network traffic between the data center and the POPs shall be encrypted.

The network design associated with the consolidated data center shall facilitate rapidly growing bandwidth and storage needs, reduce the complexity of the infrastructure, and deliver high availability (HA) and redundancy. This shall reduce the manually intensive processes and provide the convergence of networking and storage fabrics. It shall also contain standard 10Gbps and 1Gbps capabilities for attached devices, including servers, firewalls, and IPS devices.

The network shall provide a redundant topology to eliminate network downtime by a single point of failure. Contractor's network design shall provide redundancy for enhanced reliability with multiple connections to network devices. Network reliability shall be achieved through reliable equipment and network designs that are tolerant to failures and faults by reconverging rapidly to bypass faults when these occur. On a redundantly connected network, if a router fails, connectivity shall be preserved by routing traffic through a redundant connection. Furthermore, each router has two or more points, or "legs," to provide additional redundancy.

Contractor's design within the data center shall flatten the layer 2 architecture and provide a low cost capacity switching fabric. This shall be done through the adoption of a spine and leaf topology (2-tier) network design. The L2Spine is a high speed connection between any devices attached to the leaf nodes. It eliminates unused network links and introduces full throughput on all connections between network devices using Contractor's networking technology known as Intelligent Resilient Framework (IRF). Using IRF, multiple switches are grouped and appear as a single logical device that allows all links connected to these devices to forward traffic in a loop-free topology. Each device shall be fully redundant. IRF shall provide a non-blocking architecture within the layer 2 network fabric. It shall enable highly efficient high-bandwidth connectivity and N +1 redundancy. It shall provide up to 40Gbps of server connectivity to the access layer as the standard.

The data center network shall support the applications in Tulsa plus the applications that migrate from Plano. The migration moves a large amount of data across a Plano/Tulsa replication channel, but only at discrete points in time – it is not a continuous flow. Contractor shall provide the bandwidth required for each migration wave to ensure success. Contractor shall provide the bandwidth required for the Data Center consolidation, using diverse channels on the Contractor's Global Services Network (GSN) Transport. This is separate from the existing Plano/Tulsa replication circuits, and therefore has no impact on production replication traffic.

Disaster Recovery. The Tulsa data center shall be connected to the Colorado Springs DR site using a dedicated 10GB circuit, providing data replication for DR and off-site backup redundancy.

Once Contractor has tested the new network, Contractor shall cut over all the current connected equipment, as depicted by the dotted lines in the figure below. This shall be done in a planned change window, and shall be transparent to the County because all components are redundant.

Storage Architecture.

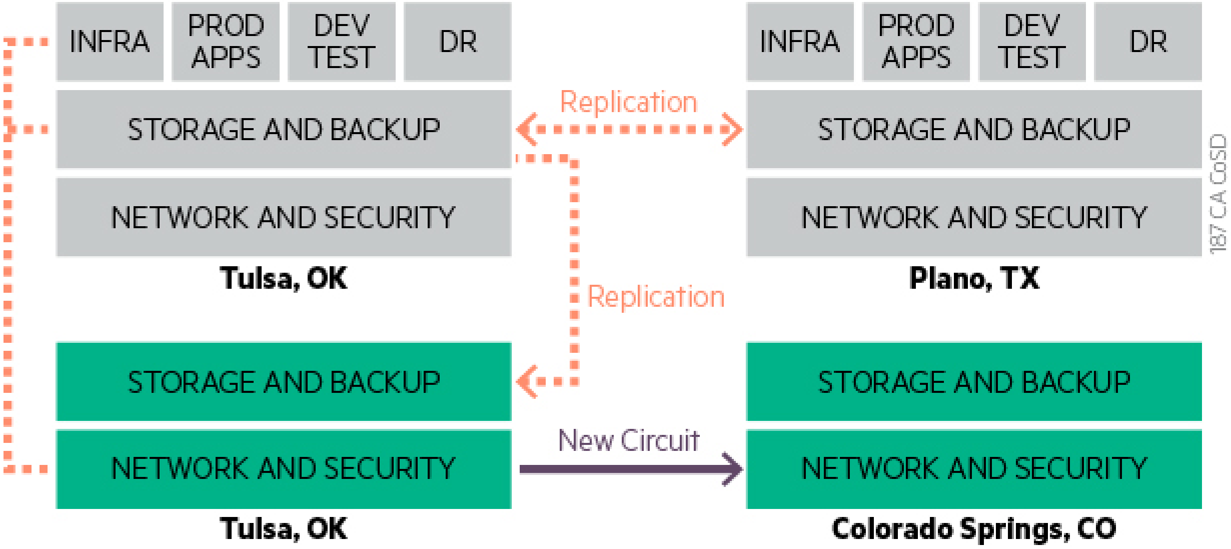
The figure below provides a view of the refresh of storage requirements:

Site	**Refresh point**
Tulsa (SAN, Immutable, VTL)	Transition
Colorado Springs (SAN, Immutable, VTL)	Transition
View Ridge & Lemon Grove (SAN)	Storage Refresh Schedule
AT&T POP (SAN)	Storage Refresh Schedule
DR POP (direct-attached only)	Server Refresh schedule

Rancho Bernardo (SAN, VTL)	Storage Refresh Schedule

The next step shall be to build out the new storage and backup equipment in Tulsa and Colorado Springs (Rancho Bernardo and other DPC sites shall have their storage refreshed on the normal refresh schedule), and start synchronizing the data between the current storage array and the new one, as shown in the figure below.

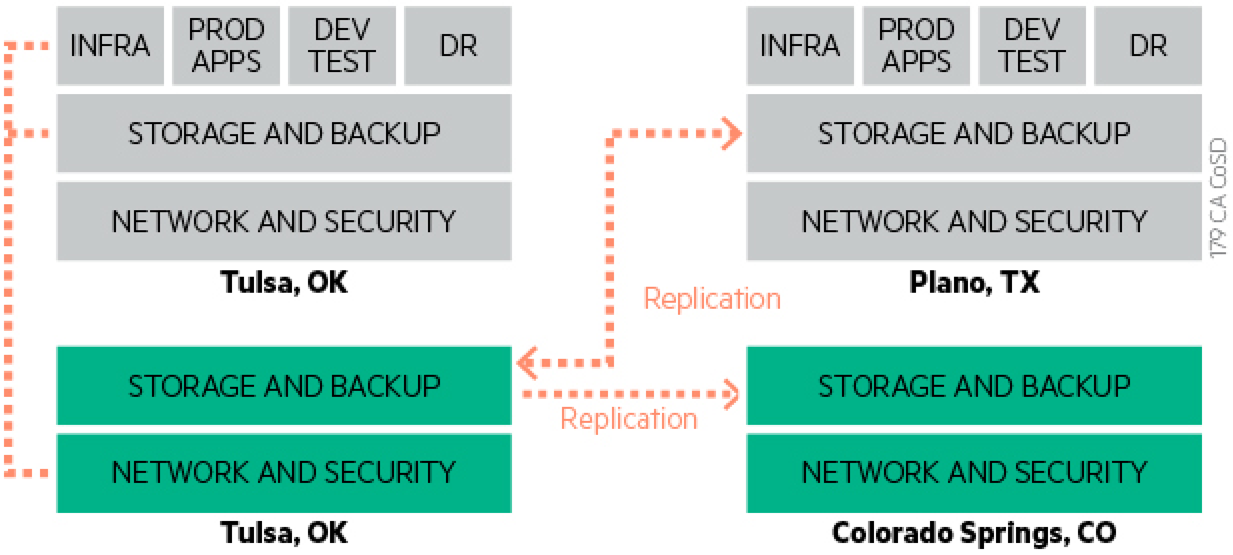
Deploying New Storage, Migrating Data



Once the new storage is fully synchronized with the current production array, Contractor shall cut over the SAN connectivity, re-initiate the replication between Tulsa and Plano, and replicate the DR data to Colorado Springs, as shown in the figure below.

In order to avoid migrating End-Users' Home drive storage twice, the County may wish to migrate this data to OneDrive for Business (ODfB) as defined in the User Data Services Transformation Project prior to the storage migration. Contractor shall accommodate this request, provided that the County can commit to supporting Contractor in achieving the ODfB migration in 6 months or less from CED (the currently planned schedule calls for 7 months), with larger move groups. If the project cannot be completed in that timeframe, Contractor and the County shall permit the Data Center consolidation to proceed on schedule anyway (i.e., do not create a dependency between the two projects) in order to avoid the risk that the Data Center Framework Transition exceeds its allowable timeline due to delays in the OneDrive migration

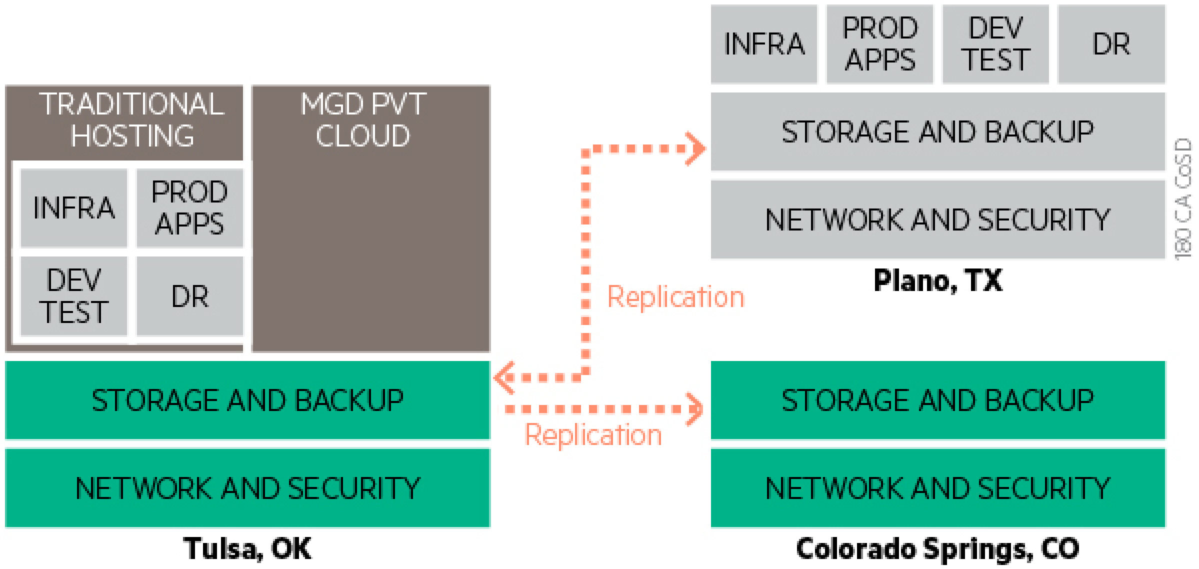
Cutover to New Storage Arrays



Then Contractor shall decommission the old storage and network environments (see figure below).

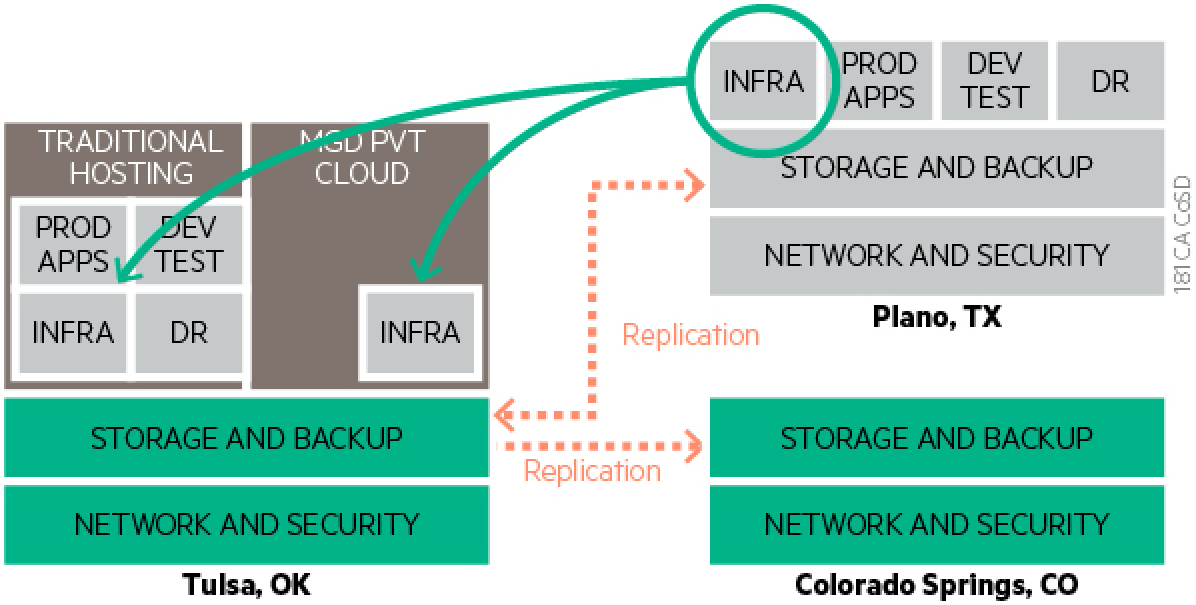
At this point, no migrations have taken place: Contractor has built out the new capacity to support the migration and the hybrid cloud architecture.

Decommission Legacy Network and Storage Hardware in Tulsa



Contractor shall build out the MPC—the County's pre-configured cloud resources—while the migration planning and detailed scheduling is taking place (see figure below).

Migration from Plano to Tulsa



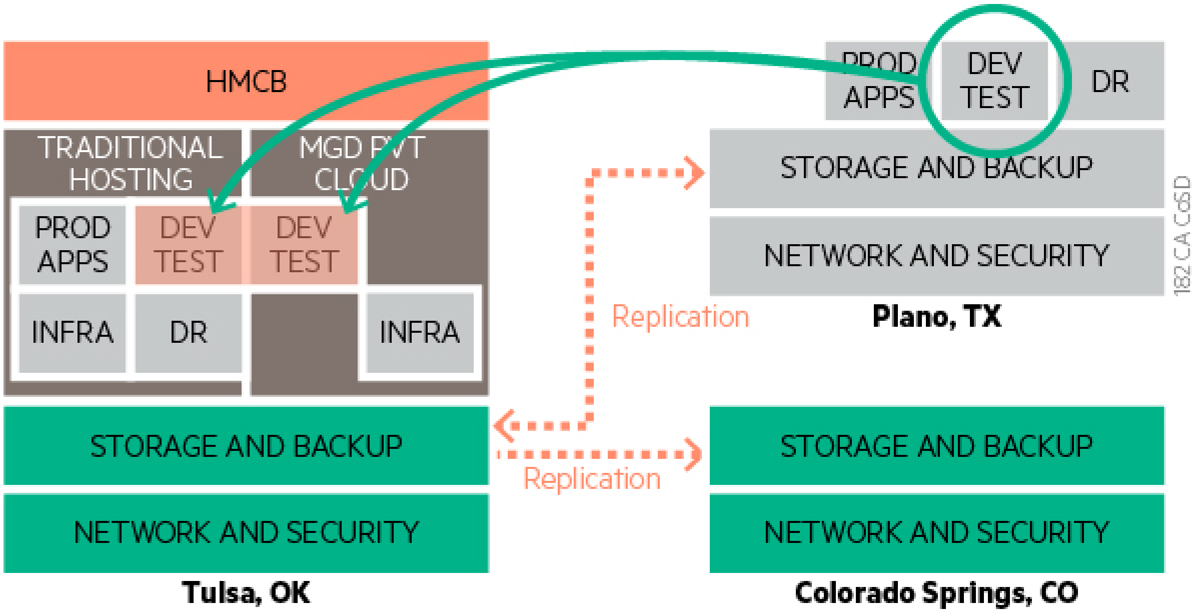
Data Center Hybrid Architecture. Contractor shall deploy hardware and software for a hybrid computing solution that supports applications and infrastructure services for the production and Dev/Test environments. The hybrid architecture shall combine a HPE Helion Managed Private Cloud (MPC) for cloud-compatible applications and traditional hosting for business applications that are not cloud-compatible, resulting in a hybrid environment. The MPC and the traditional hosted infrastructure shall accommodate the combined workloads from Plano and Tulsa, and shall be able to scale as needed to support the County's needs.

Servers with resource needs higher than the predefined sizes can be migrated into the largest size, then scaled up to meet their resource needs. Sixty percent of the servers in the data center environment are already located in Tulsa and technically do not have to move to achieve the County's consolidation goal; however, to gain the benefits of automated provisioning and the ability to turn servers up and down for Dev/Test and Applications M&O "Break/Fix" environments, Contractor has included the cost of moving those that are eligible to be hosted in MPC during the Data Center Transition, to include application regression testing. Sixty-seven percent of the servers in both Plano and Tulsa are eligible to migrate into MPC; however, per the County's request, Contractor shall not migrate the Tulsa production servers during Transition.

Contractor shall work with the application stakeholders' users to identify the best migration windows and methods for each application or related group of applications, and, depending on the platform, Contractor shall either migrate them into the Traditional hosting environment or into the MPC, as depicted in the figure below.

Building out the Cloud Broker shall take place in parallel. As Contractor creates the pool view of the Dev/Test environment, Contractor shall migrate servers from Plano into it, and either keep them live if they are P1/P2 applications or traditional infrastructure, or turn them down if they are P3-P5 in MPC and are not currently being used for a project or active M&O work. See figure below.

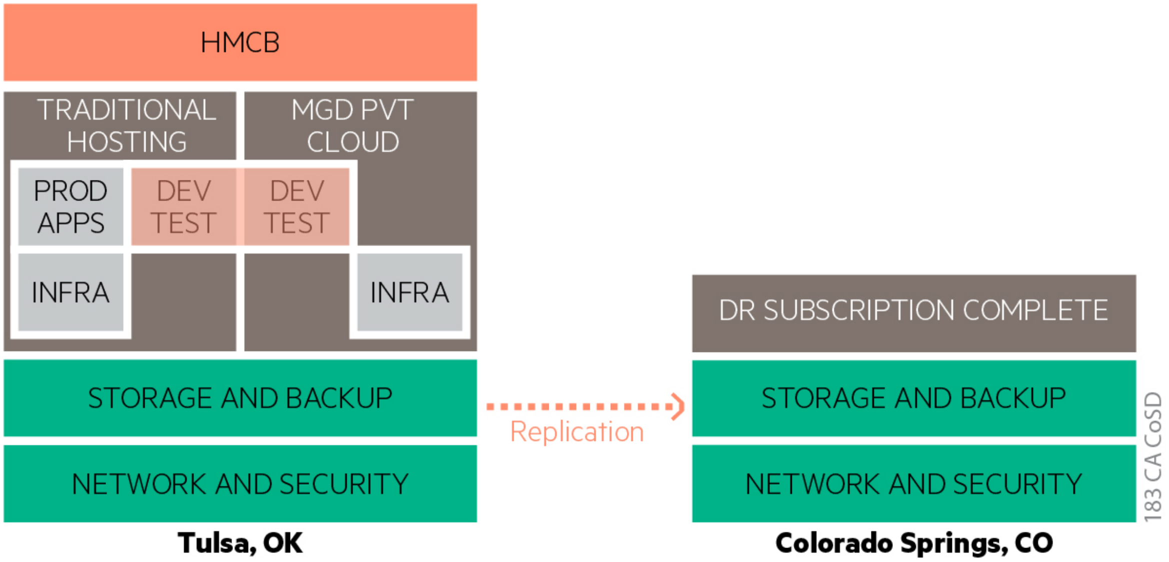
HMCB Deployment, Establishment and Migration into Resource Pools



As Contractor moves the production servers, Contractor shall make sure that their corresponding DR subscriptions are in place before the migration move group executes. That there shall be minimal changes to applications—only what is needed to facilitate the migration and redirect any Internet access from using the County's Internet at the COC and POP to the Leveraged Internet Service.

Once the migration from Plano is complete (or in parallel, as schedules permit), Contractor shall move any eligible Test and Development environments in Tulsa into the MPC. As shown in the project schedule, the migration plan and pricing include moving any eligible Tulsa server environments into the MPC; however, these moves can be deferred to the refresh timeframe, if this is the County's preference.

Future Mode of Operations



The mainframe and AS400 environments shall need to remain intact beyond the end of the Transition period. The infrastructure required to support those environments shall remain in Plano for as long as those systems are needed.

Rationale

Contractor shall enable multivendor support across hypervisors, OS instances, and infrastructure. Contractor shall provide a private cloud environment that consists of server, storage, and networking built for the cloud. It shall also consist of security, automation, and management software designed for hybrid delivery.

Contractor shall consolidate the data center workload that is currently hosted in the Contractor’s Plano, Texas data center facility into Contractor’s Tulsa, Oklahoma facility.

Contractor’s Cloud Broker solution shall provide the County with an enterprise view of all data center platforms, including private cloud, public cloud, and traditional hosting environments. The cloud broker shall give the County the ability to have an enterprise view of system performance as well as financial management across each of the hybrid platform through one pane of glass. It also shall provide a single console for provisioning compute resources across the County’s hybrid estate.

- Deployment plan for resources and use of facilities

Contractor shall assign a data center consolidation transition project manager (TPM) that shall report to the Transition Services Manager. The TPM shall have overall responsibility for this project and shall be the primary point of contact for the County in support of all data center consolidation activities. This TPM shall be responsible for maintaining the Contractor’s Move Group Plan and collaborating with the County’s designated project leader, as well as coordinating activities with the other TPMs and the Contractor Project Management Office. Contractor shall also assign a Contractor account executive sponsor to provide executive visibility throughout the project.

The data center consolidation TPM shall be directly responsible for all activities associated with the DR and storage architecture subproject activities and provide oversight of the team. The TPM shall be assisted by:

- Another TPM that shall be responsible for the buildout and testing of the cloud components
- A TPM whose focus is applications readiness, and shall work closely with the County and the Contractor team to closely manage application testing, remediation (if necessary), and scheduling priorities of the County stakeholders.

Contractor’s virtual support shall include architects, engineers, and migration specialists with specialized expertise in each of the disciplines required to deliver the various components of the plan.

The data center facilities at Tulsa, Plano, and Colorado Springs shall support transition. The transition project management teams shall be headquartered at Contractor’s Rancho Bernardo site.

- Key methodologies and processes in solution

Transition Schedule and Tasks

As described above, Contractor shall use a phased transition approach to accomplish the data center transition. For each phase, Contractor shall follow a standard process that includes an assessment of the existing environment to adjust for any changes that may have occurred as of the Contract Effective Date and the status of any in-flight projects. Each phase of the plan shall include submission of project deliverables to the County for review, response, and subsequent approval, and all approved project deliverables shall be made available to authorized users via the Service Portal.

Because the data center transition has a number of interdependencies and subprojects, Contractor shall first initiate a planning and governance phase, as part of the overall transition high-level planning sessions, which shall kickoff this set of projects.

Consolidation Assessment. In preparation for the migration of the applications from Plano, Contractor shall classify servers in terms of their migration targets and analyze server mapping.

Following the high-level planning activity, Contractor shall move directly into the detailed design and build phases. The first part of the implementation is the data center network. The draft data center network transition plan is depicted in the second figure below. An early output from the assessment shall be identification/verification of additional network bandwidth needed in the Tulsa data center. Contractor shall use this information to engineer the new network design and identify the specific network devices and configurations to be ordered and installed in Tulsa. Contractor shall submit this plan to the County for approval prior to placing equipment orders. Once approved, Contractor shall develop the final Bill of Materials and order the equipment.

With receipt of the equipment, Contractor shall begin installation of the data center network compartments in both Tulsa and Colorado Springs. In the Tulsa environment, Contractor shall create interconnects between the existing and new network infrastructure, then reroute traffic to the new or upgraded circuits. An integral part of the new network architecture is the establishment of the firewalls/IPS' and security zones needed to support traffic segregation and authorized third-party access. As part of the overall testing process, Contractor shall validate and test third-party access to the new network environment. Once testing is successful, Contractor shall move the network design deliverables to "as-built" documents, update all process documentation based on the new technologies, and submit all required deliverables to the County for review and approval.

As the network design and buildout is taking place, Contractor shall analyze the DR requirements.

As part of the Data Center Consolidation transition design process, Contractor shall seek to optimize County software licensing costs. Existing County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings. Examples of County vendors that use these types of licensing models for enterprise server software include Adobe, EMC, Microsoft, Oracle, Symantec, IBM, and VMware.

Methodologies to reduce license obligations for server/CPU/core based licenses include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment.

MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases.

Data Center Services DR Plan and DR Architecture Implementation.

During the design phase, Contractor shall review the environment specifications for the Disaster Recovery site, and shall make any updates needed. The final specification shall be conveyed to the Colorado Springs team, who shall put in place any necessary hardware and software to support the subscription contract.

Once the network connectivity between the Tulsa and Colorado Springs is established, Contractor shall begin replicating both live data and virtual tape library (VTL) data and verify that data replication is occurring accurately and as planned. At the end of the phase, Contractor shall perform three tabletop exercises of the DR plan to validate its functionality and address any deficiencies found during the exercise. Following successful completion of these exercises, at least 90 days prior to the cutover date for the data center framework, Contractor shall submit the draft DR plan for framework to the County for review and comment. Once Contractor has at least a few applications running in the Tulsa environment, Contractor shall schedule an actual failover test. Using the HPE Helion team's established DR testing methods, Contractor shall be able to conduct a failover test without forcing an actual outage to the production applications.

Data Center Hybrid Architecture and Consolidation to Tulsa

Consolidation Assessment. As described above, Contractor shall assess the Plano application and infrastructure environment to identify the migration approach for each. Contractor shall prepare a source-to-target mapping that documents each of the servers that shall be migrated along with the target server characteristics during this stage. Contractor shall also do an assessment of application requirements to the services provided by the MPC to determine compatibility. If there is a match, the application's Dev/Test and/or Break/Fix servers shall be moved into MPC. Contractor shall work collaboratively with the County's business users to determine the most appropriate solution for each application. Contractor's applications team shall review the applications targeted to migrate to verify if they have any common issues that need to be mitigated prior to migration, such as hard-coded IP addresses. If Contractor discover any issues, Contractor shall mitigate them prior to migration, using established change control procedures. From this process, Contractor shall have a clear picture of where Contractor needs new equipment and where Contractor has opportunities for reuse and for migration using a pack-and-ship approach, and can refine and adjust the target server environment solution into a design that reflects the detailed configurations.

Design and Procure Target Server Environment. Contractor shall design the hybrid environment in Tulsa to include:

- MPC and Cloud Broker (HMCB)
- Expansion of the capacity of the existing traditional infrastructure in Tulsa to accommodate workloads from Plano that require traditional hosting.

From the completed design documents, Contractor shall develop Bills of Materials and engineering documents, and submit internal purchase orders for any new hardware and software required. There shall be no additional cost beyond the Transition price for this activity.

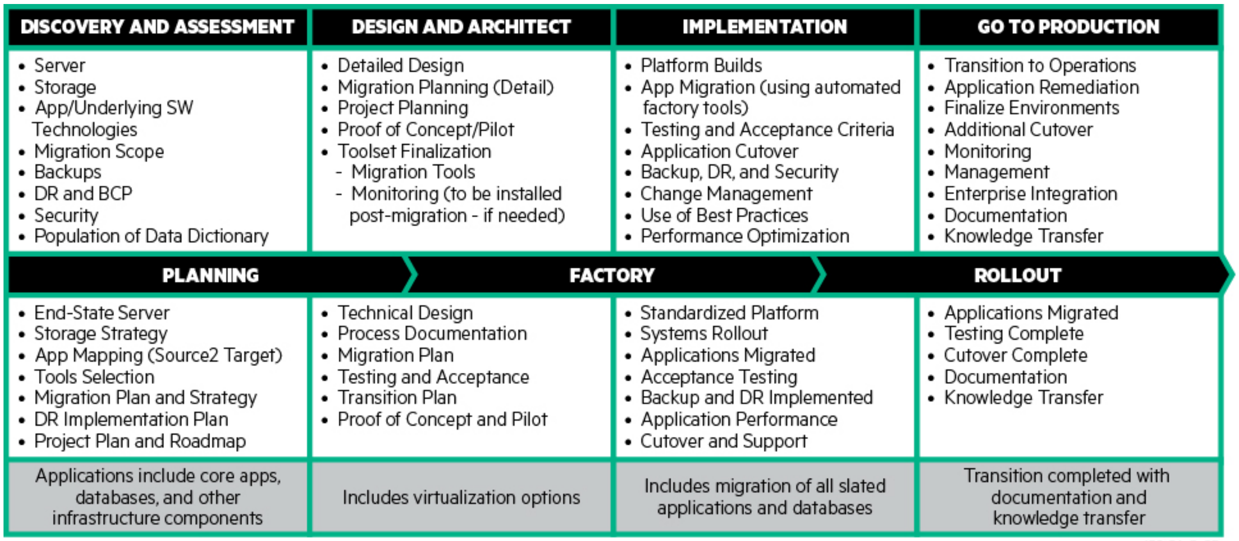
Design Migration Plan. During the design phase, Contractor shall also identify move groups that shall organize the servers according to application dependencies, and incorporate other critical factors such as the change "freeze" periods, allowable maintenance windows, and other business priorities. Contractor shall migrate all applications supporting a business process together when possible rather than migrating individual applications. Contractor shall assign a work packet for each server group supporting the same application, which shall be combined into move groups based on the critical factors identified above and application resource availability. Contractor shall create a consolidated move group plan that Contractor shall present to the County for approval.

Build-Out Hybrid Environment. The build-out of the hybrid environment shall include installing new racks, power and cabling, installing, and configuring the MPC and traditional hardware and software. Contractor shall also install and configure the HMCB. Contractor shall perform tests on the newly built servers to verify that automation processes as well as traditional connectivity and configurations to existing back-end management and reporting systems are in place, then create or update documentation for the target systems. Note that the storage architecture shall have been built out under a separate but integrated plan: at this point in time, the two schedules converge. Once the build is complete and tested, Contractor shall begin migrating move groups over the network. Tasks to build out the Dev/Test environment capabilities shall also commence during this phase.

During this time, Contractor shall work with County application stakeholders to create the detailed Migration Plan and other sub-deliverables, such as the Back Out plan, and determine the change window to execute the go-live. During this phase, Contractor shall work with and provide guidance to the County to plan the tasks and secure required resources to successfully execute the Migration Plan. Contractor shall also begin the necessary change management steps and communications processes in conjunction with the County.

Execute Migration Move Groups. An overview of the Contractor's migration methodology phases is provided in the figure below.

Migration Factory Methodology



DISCOVERY AND ASSESSMENT	DESIGN AND ARCHITECT	IMPLEMENTATION	GO TO PRODUCTION
• Server • Storage • App/Underlying SW Technologies • Migration Scope • Backups • DR and BCP • Security • Population of Data Dictionary	• Detailed Design • Migration Planning (Detail) • Project Planning • Proof of Concept/Pilot • Toolset Finalization - Migration Tools - Monitoring (to be installed post-migration - if needed)	• Platform Builds • App Migration (using automated factory tools) • Testing and Acceptance Criteria • Application Cutover • Backup, DR, and Security • Change Management • Use of Best Practices • Performance Optimization	• Transition to Operations • Application Remediation • Finalize Environments • Additional Cutover • Monitoring • Management • Enterprise Integration • Documentation • Knowledge Transfer
PLANNING	FACTORY		ROLLOUT
• End-State Server • Storage Strategy • App Mapping (Source2 Target) • Tools Selection • Migration Plan and Strategy • DR Implementation Plan • Project Plan and Roadmap	• Technical Design • Process Documentation • Migration Plan • Testing and Acceptance • Transition Plan • Proof of Concept and Pilot	• Standardized Platform • Systems Rollout • Applications Migrated • Acceptance Testing • Backup and DR Implemented • Application Performance • Cutover and Support	• Applications Migrated • Testing Complete • Cutover Complete • Documentation • Knowledge Transfer
Applications include core apps, databases, and other infrastructure components	Includes virtualization options	Includes migration of all slated applications and databases	Transition completed with documentation and knowledge transfer

159 CA CoSD

Adherence to this methodology shall enable Contractor to deliver a flawless data center consolidation.

During the assessment and design phases of the project, Contractor shall build a migration roadmap detailing the placement, design, and execution of workload migration of all workload residing in Plano and Tulsa to achieve the consolidation. Contractor shall prioritize workload migrations, with Plano workloads into Tulsa taking the highest priority. This shall allow the County to consolidate into Tulsa as quickly as possible to reduce the cost and complexity of operating in two data centers.

Pack-and-ship migrations may begin before the hybrid environment buildout is complete, if permitted by the County. If Contractor is able to ship servers before the Broker is in place, Contractor shall import those systems to the governance facility once the Broker is live to make them part of the hybrid environment.

Migration activities shall follow step-by-step processes for the Dev/Test and production environments. During this phase, Contractor shall work with the County, Contractor's technical resources, and Contractor's application SMEs to execute the migrations from the source to the target environment. The migrations shall be in accordance with the approved Migration Plan and approved detailed design documentation according to the migration schedule for each move group. The contents shall be captured in the Migration Plan developed for each application. Tasks performed as part of the Go-To-Production process, such as executing hardening scripts, loading software agents for antivirus and adding the devices to the central repository, are incorporated into the project plan to make sure that the approved Go-To-Production process is followed for all migrations.

During the migration, as assets migrate, their Resource Units shall be recast to the billing structure of this Agreement. The County shall not be billed for both in the same month.

Contractor's migration engineers, with the support of the County-designated project manager and application and infrastructure SMEs, shall execute the Migration Plan according to the project schedule. The business owner of the application shall provide the final approval during the cutover and is responsible for coordinating End-User acceptance testing and declaring the migration a success.

All migrations shall have contingency plans to invoke a back-out or other service restoration procedure in the event of a failure, or a scenario where the migration is at risk of exceeding its allotted window. The County business owner must approve any criteria for invoking the contingency plan as well as the execution of any contingency plan.

The migration plan shall include County freeze periods and adjust migration move groups accordingly, and shall consider migration alignment with maintenance windows to minimize downtime. Migration of applications impacting critical services shall be reviewed; upon County approval, Contractor may invoke the contingency plan to mitigate impact on critical service supporting County business. Each move group plan shall require County approval and participation by the application stakeholders in acceptance testing.

Automated tools like DoubleTake and PlateSpin shall help mitigate or lower the downtime considerably, as migration can be performed while source servers are live: stakeholders can test on the target servers at a time convenient for them in most cases.

- Automated systems and tools involved in solution

Contractor shall provide the migration tool licenses, such as DoubleTake and PlateSpin. Some applications may be manually installed into the target data center Following the initial seeding, the County application team shall test the application in the target data center.

Contractor's Migration Factory shall use a tool from Binary Tree Company. Contractor shall execute multiple move groups concurrently, consisting of multiple applications and associated components and using software products such as those described in the table below.

Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
DoubleTake	DoubleTake v7 is a migration tool that shall be used for migration from Plano to Tulsa. DoubleTake performs a complete server copy from the source server onto the target server. It also has an advantage of having an asynchronous replication feature, significantly simplifying the data synchronization effort required during the final go-live process. Data synchronization can be set to certain files, directories, or file systems, optimizing the amount of data being transmitted on the network.
PlateSpin	PlateSpin v11 is a migration tool similar to DoubleTake and shall be used for migrations into the County managed private cloud. PlateSpin performs a complete server copy from the source server to the target server, if needed. It allows source servers to be copied as an image that can be transported using an approved portable storage device and then restored to either a physical or virtual server on arrival at the Tulsa data center.

Storage Architecture

- Description of solution to meet the requirements

Solution Summary

The core of Contractor's primary Data Center Storage Architecture shall include the latest innovation of HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage shall host operating system images, virtual snapshots, and application data. Contractor's architecture shall enable the server image to be disassociated from the physical hardware, allowing the image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover.

The table below summarizes the types of storage in place in the County as of the Contract Effective Date, the migration technologies in use for each, and the Transition strategy for each.

Storage Transition Summary

TIER	AS OF CED	FUTURE	TRANSITION APPROACH
1 (Data Center)	3PAR P10000 thick provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thick provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
1 (AT&T POP)	3PAR StoreServ 8400 2N Solid State drives	3PAR StoreServ 8400 2N Solid State drives	No change in Transition. Contractor shall review and re-address the architecture when this storage comes due for refresh.
2	3PAR P10000 thinly provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thinly provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
Archive	3PAR P10000 thinly provisioned 7,200 RPM drives (Tulsa)	3PAR P20000 thinly provisioned 7,200 RPM drives (Tulsa)	Replication, Peer Motion
DPC	3PAR 7200 with 10,000 RPM drives	3PAR 7200 with 10,000 RPM drives	No change in Transition. Contractor shall review and re-address the architecture when this storage comes due for refresh.
Immutable	EMC Centera SN4	EMC Centera Gen4LP	Replication
Email	Email is stored on the 3PAR in both Plano and Tulsa	Provided by the Microsoft Azure Government Cloud	E2E Complete™
Mainframe	HPE P9500 or equivalent in Plano (leveraged)	HPE P9500 or equivalent in Plano (leveraged)	None. Mainframe storage remains intact until the mainframe is decommissioned. At that time, the new midrange solution for those applications that have been deployed (under a separate project) using the appropriate tiers of SAN storage.
Direct-Attached	Disk drives installed on and dedicated to a physical server (types may vary)	Disk drives installed on and dedicated to a physical server (types may vary)	None specific to the storage environment. Direct attached storage shall be replaced, and its data migrated to new storage at the time its associated server is refreshed.

TIER	AS OF CED	FUTURE	TRANSITION APPROACH
Backups (Data Center)	HPE StoreOnce B6200 Virtual Tape Library (VTL)	HPE StoreOnce B6600 Virtual Tape Library (VTL)	Replication
Backups (DPC)	HPE StoreOnce D4212 at Rancho Bernardo MSL 4048 Tape Library	HPE StoreOnce D4212 at Rancho Bernardo Replicating to DR site in lieu of tape creation, for offsite storage	No Transition of VTL environment; only need to start replication to Colorado Springs Tape Libraries shall remain intact until all tapes are expired.

The 3PAR 20000 is the latest innovation in enterprise storage from HPE. Primary data (all 3PAR-based tiers) for applications with a 48-hour Recovery Time Objective (RTO) is replicated to the DR site. The primary immutable storage shall be located in the new production data center in Tulsa on refreshed EMC Centera storage and shall be replicated to a refreshed Centera at the DR site. Contractor shall refresh the 3PAR storage at the County's San Diego sites with like 3PAR storage to reduce the impact on operational processes and maintain the same level of performance. The backup solution shall meet the requirements by providing a refreshed StoreOnce VTL in Tulsa and a smaller refreshed StoreOnce in Rancho Bernardo, both replicating to the DR site for remote storage of backup data. The backup solution changes from the current solution by replicating all data center backup data to the DR site and by eliminating remote offsite storage of backup data on tapes for the Rancho Bernardo site in favor off replicating that data to the DR site as well.

Rationale

Contractor shall meet the increased capacity and transaction requirement of the consolidated data center environment and improve the storage architecture for primary SAN storage, Contractor shall transition to a refreshed, dedicated SAN with a 3PAR 20000 storage array.

Contractor shall provide improved storage performance and capacity at the point of refresh, without disruption to County business applications. Contractor's Transition shall ensure data redundancy between Plano and Tulsa is re-established in the Colorado Springs DR site prior to removal of the Plano environment.

- Deployment plan for resources and use of facilities

Depending on the type of storage and stage of the Transition, Contractor shall execute this project at the Tulsa and Plano data centers and Contractor's Rancho Bernardo site.

Contractor's storage Transition engineers shall come from Contractor's U.S. Public Sector delivery organization, a virtual team composed of U.S. citizens based in the Continental United States, working in close coordination with the local San Diego teams.

Contractor shall engage EMC Professional Services to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

- Key methodologies and processes in solution

Contractor shall use a combination of host-based and storage-based replication to migrate data to the new storage and backup infrastructure without interruption to business processes and without data loss.

Transition Schedule and Tasks

Contractor shall adjust the schedule based on the final detailed plan.

Plan, Procure, and Engineer (Design). Contractor shall create a detailed plan and design for the new storage architecture and provide engineering documents to migrate data from the original storage solution in Plano and Tulsa to the new storage solution in Tulsa and Colorado Springs (DR). Contractor shall submit the design and plan deliverables and review them with the County. The County shall review and respond based on the agreed schedule. Contractor shall make any final revisions and create the detailed Bill of Materials from which Contractor shall procure the needed hardware, software, and services. All design deliverables shall be posted to the Service Portal as required.

Build New Storage and Backup Architecture, Enable Remote Replication. Once hardware is received, Contractor shall begin the build process. Contractor shall install the new SAN switches, storage, and VTL in Tulsa, configure and test the environment, and begin the process of replicating data from the current Plano array and VTL to the new Tulsa array and VTL. Contractor shall replicate from Plano to Tulsa throughout the Data Center Consolidation project, and replication shall be shut down for each application at the point during the consolidation when all application data has been verified and accepted on its Tulsa system.

Preparation of the DR environment shall also occur in parallel with the buildout at Tulsa. Once the DR environment is available, Contractor shall begin replication of SAN storage for applications that require DR with a 48-hour Recovery Time Objective (RTO), from the new Tulsa array to the DR site. Contractor shall replicate VTL data to the DR site for applications that require DR with a 72-hour RTO. Contractor shall begin replication of VTL data from Rancho Bernardo to the DR site for offsite storage.

Contractor shall engage EMC Professional Services to perform the Transition activities for Immutable Storage; this shall include refreshing both Centera units. The new units shall be located in Tulsa and in the Colorado Springs DR site. The new Tulsa Centera shall be configured to take over as the primary, and shall replicate to the Centera at the DR site. All existing Centera data shall be replicated to the new Tulsa Centera. The Centera refresh/migration shall not require downtime. Contractor shall reboot the Centera shortly after refresh/migration. The reboot process shall cause about one hour of downtime for the immutable storage service environment. Contractor shall coordinate this activity, like all Transition tasks, with the County via the Change Management process.

The rest of the Document Processing Center (DPC) storage and backup architecture shall be refreshed at the appropriate time post-Transition—there are no tasks required during the Transition period.

Migrate Local Data – SAN. Once the new SAN and Backup environment are fully configured and ready to support live servers, the various migrations described in the Consolidated and Single Data Center section shall begin. In addition to supporting these migrations, servers that are not migrating (that sit in Tulsa currently) shall also have their storage migrated to the new environment. There are no dependencies between the Data Center Consolidation and migration of the current Tulsa servers to the new storage—these two activities can occur in tandem.

To migrate the Tulsa environment to the new storage, Contractor shall first verify that all data is fully synchronized from the existing array. The SAN has redundant connectivity, and Contractor shall take advantage of this redundancy to move the environment from the current to the new SAN without requiring an outage to the systems or applications. Contractor shall move one set of connections from the current fabric to the new fabric, switch data access to the new fabric, then move the second set of connections to the new fabric. Contractor shall then enable replication of these volumes to the DR site.

In the new storage architecture, End-User data storage shall be provided directly from the new NAS-capable 3PAR, eliminating the need for NAS appliances. This change shall be transparent to the users.

As previously noted, Contractor and the County shall strive to migrate End-User data to OneDrive for Business in order to avoid having to migrate it to the new array as well. If the End-Users cannot commit to the four-month timeframe required, and the County does not wish to elongate the timeframe for the Data Center Framework

Transition, Contractor shall build out the End-User NAS shares by providing End-User data storage directly from the new NAS-capable 3PAR, eliminating the need for NAS appliances. This change shall be transparent to the users.

Following successful completion of the Storage Architecture Transition, Contractor shall securely destroy all data on the retired storage and backup systems and provide disposal of those items.

- Automated systems and tools involved in solution

Both the backup storage (VTL) and 3PAR shall have native replication capabilities built into and enabled by the storage array software. When host/system-based replication is used, DoubleTake V7 shall be the tool that migrates the data along with the server image. The following table lists storage-based tools and utilities.

Storage-Based Tools and Utilities

TOOL	DESCRIPTION AND USAGE
VTL Utilities	StoreOnce replication using Catalyst Replication of de-duplicated backup data reduces time and bandwidth on the dedicated replication link between Tulsa and the DR site. Backup data is available for DR more quickly, to reduce the chance of missing backup data in case of a DR event.
3PAR System Utilities	• 3PAR array-based replication allows background replication of storage from one array to another and shall aid the migration of service data from Plano to Tulsa. • 3PAR Storage Peer Motion allows Contractor to migrate storage data volumes off the old Tulsa 3PAR onto the new Tulsa 3PAR without any interruption in accessing the data.

Service Portal

- Description of solution to meet the requirements

Solution Summary

Contractor's End User Access (EUA) solution, integrated closely with Contractor's Service Management systems (Service Manager), shall provide a centralized Service Portal for all County users. Contractor's Service Portal shall provide access to self-service assistance options and multiple dashboards easily accessible by County users, Service Desk agents and Contractor support teams. It shall be mobile-enabled and easy to use.

During the Service Desk Transition, which shall occur in accordance with the Transition schedule, Contractor shall set up the core Service Portal functionality, including single sign-on, and link it to current data sources and source systems to integrate with the current repositories.

- Deployment plan for resources and use of facilities

Contractor shall assign a TPM for the Service Portal Transition Project. Contractor shall work with the County Technology Office (CTO) and its designees to assist in the design and testing and governance of the Service Portal. Contractor's Global Engineering and Technical Consulting (GETC) organization shall provide the engineering and customization work, in collaboration with the County's local engineering and support team, which manages the current portals. Contractor shall hold design sessions with the County at Contractor's Rancho Bernardo site or at a designated County location.

- Key methodologies and processes in solution

Contractor shall use infrastructure project management processes in delivery of the project.

Transition Schedule and Tasks

The following figure provides a sample view of the activities associated with the Service Portal Transition.

Design Customizations. The Portal configuration process shall be an Agile-style iterative process providing rapid feedback throughout. At the start of the project, Contractor shall collaborate with the County in several iterative workshops to design the Portal "look and feel" and to review initial functionality. The configuration process that takes place during the Transition period shall include items such as the following:

- County branding and "look-and-feel" elements on the front page (tiles, menus, links)
- Use of banners and splash pages
- Identification of End-User roles to be configured, to determine which groups have access to the various types of information
- Integration with Active Directory for Single Sign-on and configuration of End-User roles
- Integration with Service Manager and other tools
- How existing portals and data sources (ITSC, Doc Vault, and so forth) shall be presented—as links or tiles from the main page to the existing functioning applications.

Service Portal Implementation. During transition, Portal implementation has two parts: (1) the "look and feel" of the Portal and (2) integrating HPE Service Manager (SM) and other applications and data sources. Contractor shall begin with a sample portal and gather feedback from the County to determine the County's preferences. This shall be an iterative process, and once finalized and approved by the County, it shall become the Transition release design version.

With Portal design in hand, the next task shall be to connect the functionality of the document repositories and portal systems in use today to the appropriate tiles or links in the new Portal design. The integration of Service Manager with the Service Portal shall be part of Contractor's product integration. The functionality in the Portal that is embedded in Service Manager shall require minimal configuration. For Transition, there shall be no change in the application functionality of existing source applications that sit behind the Portal (those reached by pass-through links and that are not part of the Service Manager suite).

Testing. With the design complete and built, the Portal and attached functionality shall be tested. Contractor shall use the testing methods used for other infrastructure and applications releases, progressing from Systems Integration Test (SIT) through User Acceptance Test (UAT).

Content Development, Content Migration, and Training. In the same timeframe as the testing phases, Contractor shall create Service Desk related content, such as self-help content (videos, tip sheets, and so forth) and cross-functional content associated with the Service Desk available on the Portal. Contractor shall create Service Desk scripts and conduct training for the Service Desk agents to support the Service Portal, and work with the County to develop training and communications materials to introduce users to the new capabilities.

At the end of the process, Contractor shall present final documentation and the Portal itself for County review and response. Approval and successful completion of the activities above shall mark the end of the Service Desk Framework Transition. During the rest of the framework transitions, reports, updated process documentation, design documents, and other deliverables shall be posted to the Service Portal as these deliverables are completed.

- Automated systems and tools involved in solution

The Service Portal shall be customized using End-User Access (EUA) and other web development tools.

Contractor shall use Project and Portfolio Management Center (PPMC) as Contractor's Primary Project and Portfolio Management (PPM) tool suite. Contractor use PPMC for the development and ongoing management of project schedules.

9. TRANSFORMATION PROJECTS

9.1. Transformation Services

Contractor shall control transformational projects through Enterprise Architecture (EA) governance processes that incorporate CTO architecture principles, bricks, reference patterns, technology assessments, regular meetings and roadmaps to identify and align solutions suitable with County business and IT strategic direction. Contractor’s CTA and Contractor’s EA team shall continue to lead innovation days and technology seminars, focusing on improvements to keep the County moving forward. Contractor shall establish actionable roadmaps with measurable objectives to forecast and accommodate business changes in an agile orientation through effective governance and processes that:

- Use EA tools such as MEGA to create artifacts to identify, allocate, and measure transformational initiatives from an end-to-end perspective
- Establish a Transformational Maturity Model (TxMM) and analytical algorithms to analyze, predict, and recommend architectural and transformational initiatives
- Establish a Model Driven Enterprise in which service models are used to simulate and test emerging value chains and alternatives and accomplish prototyping and testing without impacting operational baselines
- Incorporate recommendations based on bi-modal organizational thinking.
- Blend bi-modal approaches to build County services from an “Outside-In” perspective.

Contractor shall leverage Contractor’s knowledge of the County environment, business processes, and strategic objectives.

- Solution Summary and Rationale

The following section sets forth Contractor’s approach to addressing the individual Transformation Projects, as listed in the table below. These projects shall be undertaken at the County’s request, follow standard Service Request procedures, and shall include no less than what is described in this Transformation section.

Transformation Projects

TRANSFORMATION PROJECTS
Desktop Services
User Data Services
IT Application Portfolio Management Services
Network Transformation
Voice Services Transformation
Storage Architecture
E911
Identity Federated Services
Enterprise Information Management (EIM)
Comprehensive Applications Threat Analysis (CATA) Service

Desktop Services Transformation Project

- Solution Summary & Rationale – Description of solution to meet the requirements

At County’s election, Contractor shall implement Presentation Virtualization (also known as Application Virtualization) driven by Citrix XenApp. Presentation Virtualization helps address the need by decoupling the legacy applications from the device in such a way that it minimizes the infrastructure and overall costs when compared to other virtualization approaches. In doing this, legacy applications no longer dictate the upgrade path for the rest of the County’s environment and this minimizes the potential for impact if a particular application such as Kronos, Acclaim, or Accela causes problems with the latest O/S upgrade, or browser version. This, and all of the other virtualized apps, can remain for as long as the County continues to use the apps. Transformation of legacy apps can then proceed on their own timeline, rather than being tied to the remainder of the IT environment.

Each virtualization option, illustrated in the Compute Style section of the figure below, is generally related to a specific type of End-User’s digital profile, and is typically based on their overall work related IT requirements (e.g. Device(s), Applications, Data, and Support). As the need for more computing power increases (i.e. CPU, Memory, graphics) at the End-User level, the more complex and costly the virtualization solution becomes.

Project Deliverables:

- Virtualization of up to 200 County applications
  - For up to 15,000 County Users

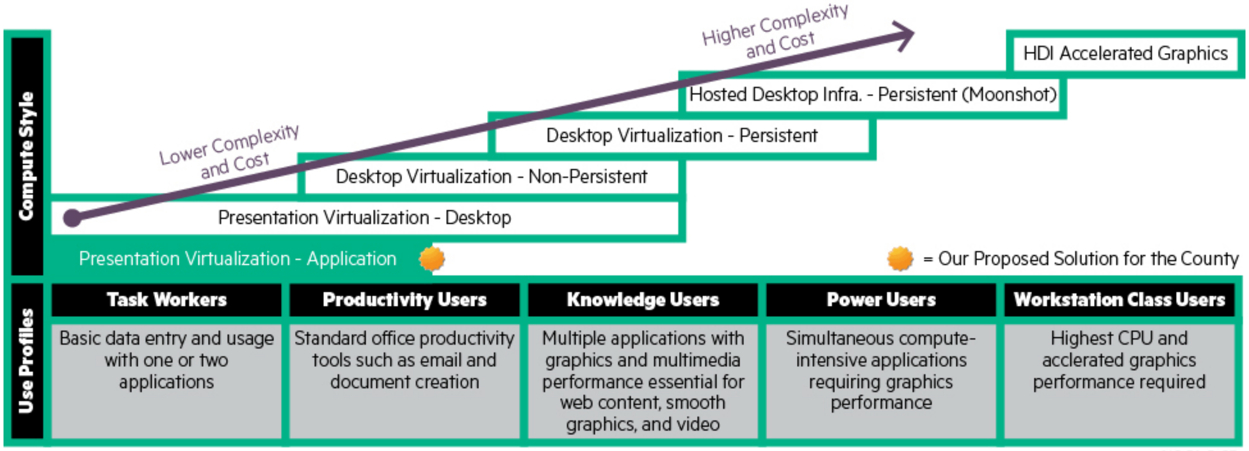
Contractor assumes High Concurrency of End-Users, meaning that for the most part, multiple users would be accessing the application(s) at the same time.

Client virtualization processing load is not only determined by the number of concurrent users, but by the complexity of their applications. The greater the application complexity, the lower the End-User density per server. As a result, application complexity is an important determinant of the number of concurrent users that can be supported on a given Client Virtualization Service (CVS) solution. Contractor classifies application complexity into three groups: light, medium, and complex and has assumed an application profile of medium complexity for the County. Medium Complexity is a standalone application that has minor dependencies on the OS, a prerequisite application, or large/complex data feeds. Most business-related common off-the-shelf applications are considered medium complexity. One notable exception is Microsoft Excel workbooks with embedded macros that can be considered complex in nature.

Specific deliverables include:

- CVS design assessment
- Detailed Presentation Virtualization solution design
- Implementation of the approved solution
- Standardized Contractor CVS Presentation Virtualization monthly reports.

Presentation Virtualization


Compute Style
Higher Complexity and Cost
HDI Accelerated Graphics
Hosted Desktop Infra. - Persistent (Moonshot)
Desktop Virtualization - Persistent
Lower Complexity and Cost
Desktop Virtualization - Non-Persistent
Presentation Virtualization - Desktop
Presentation Virtualization - Application
= Our Proposed Solution for the County
Use Profiles

Task Workers	Productivity Users	Knowledge Users	Power Users	Workstation Class Users
Basic data entry and usage with one or two applications	Standard office productivity tools such as email and document creation	Multiple applications with graphics and multimedia performance essential for web content, smooth graphics, and video	Simultaneous compute-intensive applications requiring graphics performance	Highest CPU and accelerated graphics performance required

142 CA CoSD

The approach decouples the legacy applications from the device in a way which minimizes the infrastructure and overall costs compared to other virtualization approaches.

Rationale: Presentation Virtualization, provides all the required functionality and is significantly more cost-effective than other solutions, such as VDI (i.e. Desktop Virtualization, both non-persistent and persistent). Contractor recommends a periodic re-evaluation of Client Virtualization after a number of years, perhaps making the next step to VDI if the requirements change, and if it makes sense financially for the County. This would also be a time to review the current desktop build from the ground up, since VDI would require a much thinner client.

Contractor designed the solution for the County to use the same software stack and versions to deploy and to manage it throughout the life of the Agreement. The solution includes:

- Lakeside Software's SysTrack (for Assessment)
- Citrix: XenApp, XenServer, NetScaler
- Microsoft Server, SQL
- AppSense DesktopNOW Environment Manager.
- Liquidware Labs ‘Stratusphere™ UX’, Profile Unity and FlexApp
- HPE’s Standard Reference Architecture
- Automated Tools – Automated systems and tools involved in solution

Contractor’s analysis shows that typically 80 to 90 percent of the use cases can be met by presentation virtualization (typically Citrix XenApp). Presentation virtualization is the most cost effective way to deliver legacy applications when compared to other desktop virtualization technologies, including VMware solutions.

Desktop product upgrades or changes to the Applications Portfolio require significant time and engineering efforts to deploy. Presentation virtualization addresses this issue in that upgrade engineering and testing need only focus on one image: that of the server in the data center running the application that is being presented to the End-User. Virtualizing desktop applications removes a dependency on various desktop client hardware.

This helps prevent deployment delays and post-deployment problems while improving the ability to rapidly maintain desktop currency, at least for the many desktop applications that are virtualized.

Presentation virtualization shall also help maximize the performance of all the applications on the End-User device, whether virtualized or local.

Timing: The Presentation Virtualization project would follow Transition completion.

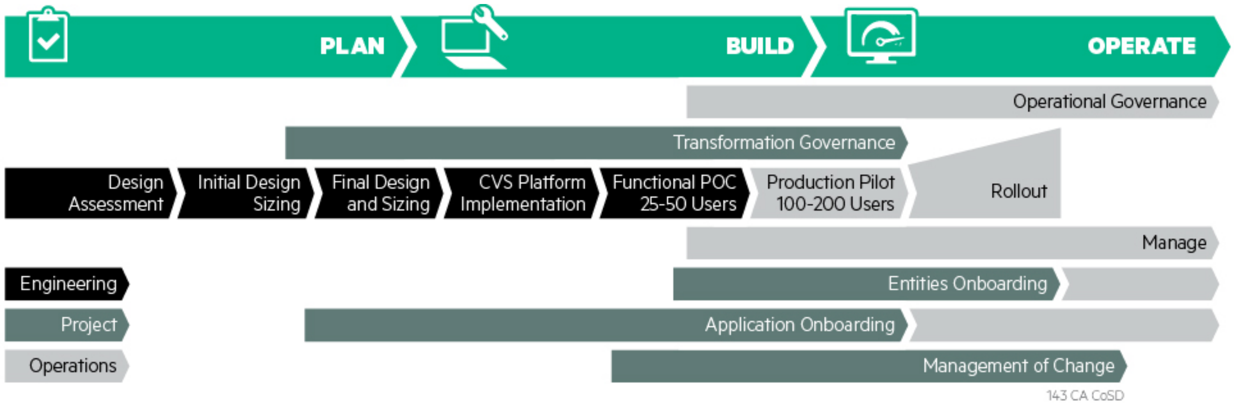
Risk Considerations: The introduction of client virtualization changes the way users perform their work and is therefore considered disruptive. Failed first attempts to introduce users to client virtualization result in roll-out delays, onboarding program rework and reintroduction to users which is costly, time consuming and can significantly erode the expected ROI. For a high degree of success, consider the following:

- **Entity onboarding -** Depending on the structure of the customer and according to the priorities defined during the assessment/analysis/design phase, Contractor recommends ramping up users by personas (groups of users). End-User personas could be a business unit, a department, a typical group of End-User profiles based on common desktop or application requirements. This involves identifying people, managing the persona grouping, desktop and application group entitlements and orchestrating this by means of Active Directory.
- **User onboarding -** Onboarding management and Client Virtualization Service (CVS) Management links the two onboarding subphases (Entity and User onboarding). Contractor proposes to migrate a category of virtualized users either by a specific persona and/or with relatively similar desktop/application requirements, and begin with less complex use cases then progress to the more complex. Subsequently, the scope will be increased until all users have been on-boarded successfully.

All onboarding activities are managed and controlled by an onboarding manager. Once users are successfully onboard in the production environment, they are managed like any other End-User with a CVS Service Manager. The CVS Service Manager monitors the overall performance of the virtualization service, coordinating performance review meetings and reports with both the customer and CVS operations.

Key dependencies and Milestones: Contractor's proposed deployment is comprised of two discrete parts, with the second part dependent upon completion of the first. These are CVS design assessment and implementation.

Representative Key Milestones for a Presentation Virtualization Deployment



Durations and dates of the major tasks are dependent upon the data gathered from the first step, the Design Assessment. After the Design Assessment, Contractor develops the final implementation timeline. Typical Presentation Virtualization projects of similar complexity to the County's take approximately five months.

- Deployment plan for resources and use of facilities

The following Contractor resources shall support this transformation project:

- The Contractor Workplace Transformation Consulting Team shall perform the CV Assessment
- The Contractor implementation team consists of
  - An overall Program Lead that is a subject matter expert (SME) in End-User Compute solutions.
  - Additional SMEs based on the overall solution scope and may include but is not limited to: project management, deployment and implementation planning, infrastructure specialists, End-User onboarding, training, Image Creation / Mgmt., application packaging and testing.

- A senior Transformation Manager who is responsible for the end-to-end project scope and stays in place until acceptance criteria have been met.
- Ongoing support for the Presentation Virtualization service shall be delivered by US-based delivery resources in line with the County's requirements.

- Methodology & Key Processes – Key methodologies and processes in solution

Contractor follows a proven methodology for CVS implementation that begins with the CVS Design Assessment, and continues through implementation and ongoing management as described below.

CVS Design Assessment: Contractor shall assess a sample of existing County users, looking at how they interact with their apps and analyze how the apps interact with users' devices. This helps the appropriate applications for each End-User type to be identified and drive the transition plan from the current mode of operation (CMO) to the desired future mode of operation (FMO). This assessment would take into consideration the following items:

- The desktops included would be a sample of End-User desktops for each type of user and IT usage
- A "Type of End-User" categorization, which refers to the type of applications users work with the intensity with which they use them as measured by CPU, RAM, disk IO, and network traffic
- A "Type of usage" categorization, which includes not only the PC, laptop, tablet, smartphone, or engineering workstation each End-User needs to do his/her job, but also any requirements for peripherals such as USB connected security dongles, portable data storage, cameras, meters, and other specialized devices. The goal is to identify the subset of IT usage that provides the majority of business value, identify a solution that meets the core requirements for providing that business value, and, after the core requirements are met, identify how to support all other candidates for virtualization for the optimum incremental cost.

There are three steps to the Design Assessment:

- Startup
  - Developing a statement of requirements to confirm that the engagement team understands the purpose of this engagement from the County's point-of-view
  - Developing a data collection plan that details how the engagement would collect the data needed for this assessment: The purpose of this plan is to enable County personnel responsible for change management and information security to approve the data collection.
- Execution
  - Meeting notes from a discussion of the County's intended future mode of operation (FMO) to confirm that engagement team understands the desired outcome
  - An assessment report that summarizes and analyzes the collected data: The engagement team would review this assessment with County stakeholders
- Closedown
  - A solution document that identifies the next steps that the County and engagement team have jointly recommended as a result of reviewing the assessment report.

This assessment validates the initial assumptions or identifies necessary modifications of the initial assumptions related to the original scope for this effort. This revised scope, based on the data that was gathered and analyzed, can affect the original solution and can have an impact on the overall solution components including; infrastructure, labor and software that is required for the solution.

CVS Implementation: At the start of the implementation phase of the project, Contractor holds a workshop to begin the planning process. Contractor would work collaboratively with the County to identify and agree upon key milestones and objectives, and Contractor would report status on these throughout the implementation.

Contractor has an established and proven transformation methodology that follows an industrialized "factory" approach. This methodology is organized in phases, as described in the following overview, with clear milestones that are established by Contractor and the County after the Design Assessment. Contractor then creates a mutually agreed to transition plan with a detailed work breakdown structure, milestones and owners for execution.

The activities executed during the Implementation Phase of the project are:

- Design Sizing (Initial, Final)
    - Review of assessment data (End-User usage, application usage, network, End-User data, security)
    - Architecture Design and Infrastructure Implementation Plan established
- Infrastructure Set-up
    - Site preparation in the Tulsa data center and equipment provisioning. This environment can be implemented as an expansion to the County's MPC environment, or as a standalone virtual infrastructure under the HMCB, in order to integrate it with the County's hybrid cloud.
    - Server installation (HW and operating system)
    - Server integration in the County's Active Directory Domain
    - Server integration in the Tulsa data center and linkage to other infrastructure service (DNS, Storage, proxy, AV system, etc.)
    - Software implementation and configuration
- Functional Testing
    - Functional pilot or Proof of Concept (POC), is performed by a small group of IT users to verify compliance (to functional and technical requirements) and performance of the solution, and tune the configuration if necessary.
- Production Pilot
    - While the functional testing above is focused on IT users with client virtualization familiarity, this testing phase focuses on the general End-User population with the goal of testing both the technical solution and the roll-out plans and materials.
    - The Production pilot is performed with 100 to 200 selected users operating in the production environment. This pilot is for a fixed, short period of time. Test scripts are supplied to pilot users that identify the specific activities a participant is to perform. Contractor then examines the results for faults and provide feedback to the delivery team. Contractor corrects any faults, either by correcting the script, End-User performance of the script or infrastructure/software correction. Once corrections are in place, Contractor would re-run the script until all test scripts are successfully completed with no issues.
- Onboarding
    - During this phase, Contractor manages two kinds of onboarding (Entity and User, as mentioned above), each of which potentially influence the other. Workgroup/departmental similarity in application use, security, and the County's implementation priorities are the main factors in identifying a roll-out plan.
- Management of Change
    - Throughout the entire pilot and rollout period, the Transformation Manager would work with the implementation team and the operational support team to verify that the rollout plans are communicated, support is in place and End-User issues are addressed.

User Data Services Transformation Project

- Key Considerations and Potential Alternative Approaches

One of the steps to achieving a truly mobile workforce is to separate the data from the device. By doing so, County employees would be able to access the data necessary for their job from any number of devices, whether County-owned or through Bring Your Own Device (BYOD), or even via the Web. Knowing this, Contractor has formulated a number of key considerations. The solution must have the following characteristics:

- Be secure
- Allow End-User data to be decoupled from the End-User's device
- Take advantage of existing licensed solutions, tools, and services
- Allow various levels of access.

- Support collaboration both within the organization and external to it.
- Finally, County users span many different types of work, and they are multi-generational as well. Because of this, Contractor's solution balances a new way of interacting with one's data along with the need to maintain some form of familiarity.

- Description of solution

Contractor recommends taking full advantage of the technology the County already has using the County's Office 365 subscription and OneDrive for Business.

OneDrive for Business includes apps for smartphones, and allows mobile access through the mobile device management (MDM) solution.

As subscribers to the G3 level of Office 365, each End-User has 1TB of space on their OneDrive for Business account. Microsoft research shows that the vast majority of business users consume much less than 1TB Contractor's research on the County's historical use of file shares supports this. The entire size of County network shares is 78TB for all 15,000 users. Contractor would continue to work with Microsoft to facilitate optimal configurations.

End-Users can collaborate in several ways. Using OneDrive for Business, an End-User can share a document or series of documents from their own OneDrive for Business data space. The documents themselves are not delivered to the other End-User. Rather, a link to that document allows the designated End-User (and no one else, besides the owner) access to only the documents the owner wants to share.

Departments or divisions that want to have a shared space for their exclusive use can create "groups." Access to these groups is initially fully locked down. The owner of the group would have to explicitly invite members to use the shared space.

To fully realize the benefits of Office 365, users must make the move from using network file shares to storing their data on OneDrive for Business. Contractor proposes a project to migrate data on End-User network file shares to their OneDrive for Business location. The project steps at a high-level are:

- **Group Policies / Powershell Scripting.** The moves would be automated via Powershell scripts and actioned via group policies.
- **Search for invalid files/folders and cleanup.** OneDrive for Business has different requirements for filenames and folder structures than Windows. Contractor would need to locate the files that would not move in their original states.
- **Pilot.** Contractor would migrate a test group of users via automated processes.
- **Scheduling.** The migration would need to occur in waves. The project plan assumes a conservatively low size of 300 users per wave. As the waves progress, the size of subsequent waves might grow, thereby shortening the project.
- **Communication / Training.** OneDrive for Business is a paradigm shift from the traditional way of interacting with data files. Contractor would develop and deliver a communication plan as well as training for users who migrate to OneDrive.
- **Migration (waves).** The migration would occur in waves, with support throughout the entire project. At the end of the project, all County users would have completed a migration from a network share data to their OneDrive for Business account.

- Deployment plan for resources and use of facilities

For OneDrive for Business, all data is stored in Microsoft's Government Community Cloud.

Support for OneDrive for Business would come from the Service Desk. OneDrive for Business issues would take advantage of Contractor's enhanced support for Office 365 service, which uses Contractor support resources working on-site with Microsoft Office 365 support engineers.

- Methodology & Key Processes – Key methodologies and processes in solution

Contractor supports OneDrive for Business, using time-tested infrastructure processes of both HPE and Microsoft, which emphasize delivering measurable, repeatable, and efficient services to the End-User.

- Automated Tools – Automated systems and tools involved in solution

For the rollout and subsequent maintenance of the End-User device connectivity to OneDrive for Business, Contractor would use Group Policy through Microsoft System Center Configuration Manager (SCCM). This would allow a smooth rollout of the solution and would make subsequent revisions for new requirements easier as well.

- Qualifications and Experience – Background and experience in comparable environments

Internally, Contractor has transitioned ~300,000 users (HPE/HPI combined) to OneDrive for Business, using it for individual storage, collaboration, sharing, and device backup. Contractor would follow a similar process to successfully migrate the County to the OneDrive for Business solution.

This solution takes advantage of Contractor's 30-year history of partnership and collaboration where Contractor is the only Microsoft partner to have co-located shared support resources for Office 365 for the exclusive use of Contractor's customers.

IT Application Portfolio Management Services Transformation Project

- Key Considerations and Potential Alternative Approaches
-

IT Application Portfolio Management supports the continuous assessment of IT application portfolios to:

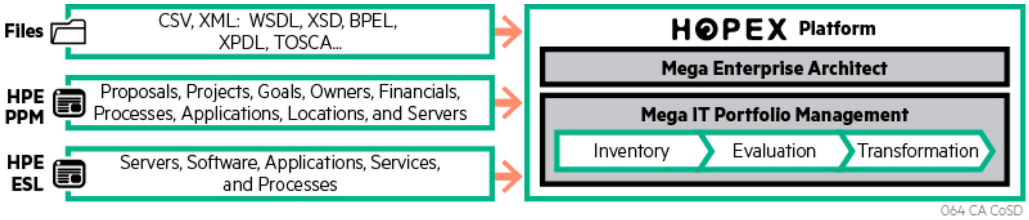
- Standardize portfolio management
- Align the IT application portfolio with business strategies
- Reduce deployment time
- Improve operational efficiencies
- Reduce costs and optimize value
- Increase visibility and understanding of the application portfolio

Key considerations for this transformation project require selecting a tool suitable for meeting the criteria listed below.

- Highly configurable
- Integrated environment
- Integration with source systems
- Speed of implementation
- Develop architecture disciplines to maximize in-place tools
- Business capability mapping
- Incorporation of application portfolio inventory
- Define cost elements
- Project-related information
- Rationalization alternatives/recommendations

- Solution Summary & Rationale – Description of solution to meet the requirements **Solution:** MEGA's HOPEX platform offers a comprehensive, well-rounded, feature-rich platform that provides an out-of-the-box metamodel that is highly configurable and has strong modeling capabilities. It also supports a wide range of industry frameworks. HOPEX combines industry-leading practices in enterprise architecture (EA), IT portfolio management (ITPM), business process analysis (BPA), and governance, risk, and compliance (GRC) into a single platform. This integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation as shown in the figure below.

MEGA IT Portfolio Management


Files
CSV, XML: WSDL, XSD, BPEL, XPDL, TOSCA...
HPE PPM
Proposals, Projects, Goals, Owners, Financials, Processes, Applications, Locations, and Servers
HPE ESL
Servers, Software, Applications, Services, and Processes
HOPEX Platform
Mega Enterprise Architect
Mega IT Portfolio Management
Inventory
Evaluation
Transformation
064 CA CoSD

This fully integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation.

Use of this tool facilitates creation of a complete inventory of IT assets, including applications, underlying technologies, and servers. Both out-of-the-box and custom reports provide information that makes it easy to evaluate IT assets using multi-criteria analysis such as costs, risks, technical efficiency, and business value, bringing visibility to the County's IT portfolio. This information also provides insight about dependencies and helps to identify redundancies of IT systems while reducing costs and complexity by eliminating systems with the same functionality. MEGA also provides the ability to create and compare multiple transformation scenarios that take into account various criteria to select the most relevant scenario for their business needs and constraints.

Upon approval from the County to proceed with this transformation project, Contractor and MEGA consultants would schedule a project planning and kickoff meeting. A topic of discussion for this meeting would be identification of County stakeholders that requested to participate in requirements gathering sessions to make certain the MEGA ITPM is configured correctly to meet the requirements.

Once in place, MEGA ITPM provides a three-step approach to managing IT assets:

1. **Inventory**: ITPM automates the collection of IT assets through a web-based interface. It provides metadata that can describe IT assets through various parameters such as functional scope, lifecycle, costs, and risks, providing a comprehensive view of the existing IT portfolio.

The inventory creation would use MEGA's APIs to interface with the ESL, partner systems, and other feeder systems (i.e., AppsManager) to make certain accurate data is in place. Once the inventory data is populated, IT assets can be viewed by business lines, business processes, business capabilities, organizational units, and technology vendors.

2. **Evaluation**: This step assesses IT assets through either out-of-the-box or custom criteria such as costs, risks, business value, and functional support. It provides detailed analysis through cost, dependency, and impact reports (i.e., brick's compliance). To rationalize the portfolio, it provides insight into which IT assets need to be removed, replaced, or maintained. Using business capability maps, IT assets are organized by functional areas, and changes are displayed over time, helping to make better-informed decisions.

Also during this step, costs and other project-related information are associated with the assets. The IT assets are evaluated by business value, functional support, and technical efficiency through the use of IT portfolio evaluation campaigns.

3. **Transformation**: In this step, the County can define a mix of initiatives or assumptions such as extending, replacing, or phasing out applications and technologies and compile them into different scenarios. The County can then assess and compare these scenarios through various criteria such as risk to quality, risk to feasibility, and costs and then identify the best transformation scenario to implement.

Rationale: Contractor has designed this project based on the recommendations of the MEGA ITPM tool product supplier, with the following characteristics and caveats:

- As requirements evolve, additional MEGA modules, such as Enterprise Architecture and Governance, may be required.
- Information from the Contractor's ESL, PPM, and AppsManager would be maintained by the source systems and would be updated by MEGA at scheduled times.
- MEGA out-of-the box functionality would be used for this effort.
- Contractor would install, configure, and manage MEGA modules.
- Licenses are included for MEGA HOPEX WorkBench and ITPM module for 30 contributors, 10 Portfolio Managers (GITMs) and 5 Advanced Users (CTO).

Timing: Contractor proposes to use the MEGA Quick Start program for implementation of MEGA ITPM. In the MEGA Quick Start program, Contractor would collaborate with MEGA consultants to conduct a project kickoff that includes the definition of project scope and schedule. Typical installation and configuration of a MEGA project takes about 45 days, including installing and configuring MEGA ITPM, conducting functional/deployment specifications workshops, designing supporting MEGA metamodels, testing the changes, reviewing and mapping the artifacts, uploading the artifacts, establishing portfolios and hierarchies, and training supervisors and users.

Risk considerations: Potential risks that could affect the project include the following:

- Automating APIs and metamodels shall require configuration and potential connector development to accommodate integration with external systems of record: AppsManager, PPM, and HPE's ESL.

Key Dependencies and Milestones: Following are the key milestones and dependencies for the project:

- Kickoff: Receipt of County approval to begin would initiate kickoff of the engagement. After the kickoff session, Contractor would define the project scope and develop the schedule.
- Installation: The next milestone is installation of MEGA on the established infrastructure. This is dependent on the availability of SQL Server licenses and availability of the infrastructure.
- Specification: The next milestone is conducting and delivering the functional/deployment specifications workshop. Part of this deliverable would be demonstration of MEGA ITPM capabilities. Contractor would prepare an ITPM customer guide. The deliverable would include the functional/deployment specifications and customer guide. This task is dependent on availability of the designated County users who would provide the requirements for use of the MEGA system.
- Configuration: The next milestone is reached when the configuration and customization of MEGA is completed using the functional/deployment specification as defined above. During this step, the supporting MEGA metamodels would be designed, built, tested, and implemented.
- Artifacts: The next milestone is reached when all artifacts are uploaded in MEGA after reviewing and mapping the ITPM specific artifacts. The portfolios and hierarchies would also be established during this cycle. At this time Contractor performs acceptance testing to verify that it is set up correctly.

- Training: This milestone would be followed by a training session for users.

- Deployment plan for resources and use of facilities

Resources: For implementation of the MEGA ITPM toolset, Contractor would use MEGA's Quick Start program. MEGA's experienced consultants would work with Contractor to install, configure, and set up the MEGA environment. MEGA consultants and Contractor staff would work with County staff to demonstrate MEGA HOPEX functionality, determine functional and deployment needs, and document the supporting requirements. To minimize the County's time investment while maximizing impact, Contractor would conduct information gathering workshops through a series of focused discussions with stakeholders to make certain that Contractor has an accurate understanding of the County's needs. At the end of this effort, Contractor would deliver a functional deployment specification and an End-User guide. Contractor would then help design MEGA metamodels and make the configuration changes to interface with PPM, ESL and AppsManager systems. Contractor would then upload the artifacts and establish portfolios and hierarchies in accordance with the County's needs. Contractor's team would also provide training for the End-User groups who would use MEGA ITPM toolset.

The Contractor team supporting the MEGA toolset would work closely with CTO, and supporting staff to provide a collaborative working environment. This would enable direct communication and provide the County with the ability to reach out directly to Contractor personnel for quick resolution of any issues.

Facility: Contractor would locate the MEGA infrastructure in the Tulsa data center.

- Key methodologies and processes in solution

Contractor would perform the installation, configuration, and management of the MEGA ITPM toolset using ITIL v3 processes, consistent with the established processes for managing County assets. Contractor would use Contractor's system development life cycle (SDLC) processes in collaboration with the County staff to configure and make necessary updates to MEGA application programming interfaces (APIs) to align with automated systems and tools involved in Contractor's solution.

The MEGA ITPM tool provides all required functionality to meet the County's requirements, and it would integrate with AppsManager, PPM and the ESL solution.

Network Transformation Project

- Description of solution to meet the requirements

The Contractor's approach to network transformation leverages the existing investment that the County has made in its infrastructure, building on the robust, geo-redundant network core to enable new service adoption while Contractor migrates from legacy technology. This foundation positions the County to make smart, progressive choices in the way services are delivered to its employees and constituents, regardless of their location or access device. As the County network continues to evolve, Contractor's ability to provide ubiquitous connectivity with seamless accessibility, security, and performance would provide the benchmark of Contractor's framework.

Cloud Enablement via NetBond

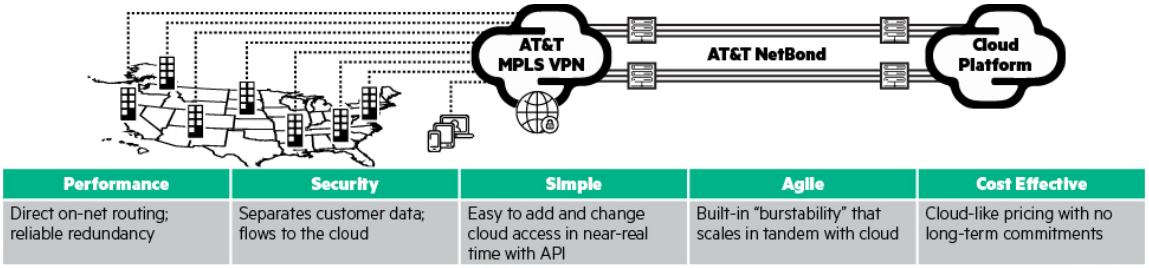
As cloud-based services mature and become more viable for Government use, Contractor is positioning the County's network perimeter to enable seamless, secure, and performance-assured integration for cloud providers. Contractor shall cause AT&T to build a geo-redundant core network foundation to enable this shift in services, leveraging AT&T's virtual private network (AVPN) MPLS-based transport. This foundation is to be deployed as a Transformation activity in preparation for future services.

Building on Contractor's AVPN transport, AT&T's optional NetBond service would be made available on a per cloud provider basis, enabling secure, performance-assured cloud-to-enterprise peering, in turn isolating these important services away from the unsecure and potentially congestion-prone Internet Service Provider (ISP) links. The NetBond service is represented as a proposed new RU, where the County can select peering relationships with designated cloud providers on a bandwidth scaling basis. Cloud provider side costs may apply and would be priced as new RUs when establishing a new cloud provider contract, as requested by the County.

AT&T's NetBond service would terminate at the County's edge, providing a geo-redundant presence in line with stated objectives; coupled with the inherent redundancy of the Global AT&T Multiprotocol Label Switching (MPLS) infrastructure, NetBond would provide the highest available level of resiliency, to enable the continuity of the County presence and its ability to conduct business.

In support of the transition of Exchange to the O365 cloud, AT&T would enable Netbond functionality in a peering arrangement with Microsoft's ExpressRoute product. This would be designed and implemented in line with the specified transition plan and is priced as a separate resource unit that combines the NetBond RU with the ExpressRoute costs to complete the connectivity model for the service.

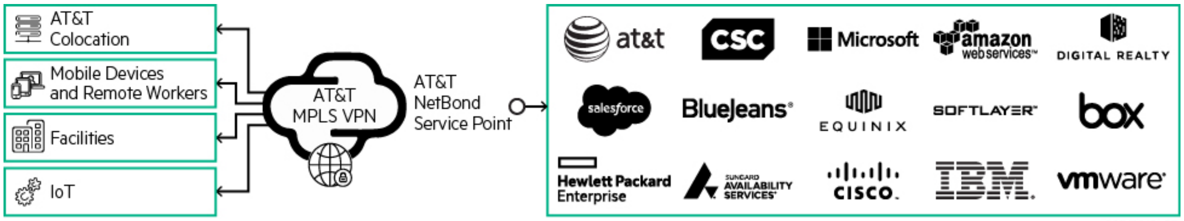
AT&T NetBond Benefits



Performance	Security	Simple	Agile	Cost Effective
Direct on-net routing; reliable redundancy	Separates customer data; flows to the cloud	Easy to add and change cloud access in near-real time with API	Built-in "burstability" that scales in tandem with cloud	Cloud-like pricing with no long-term commitments

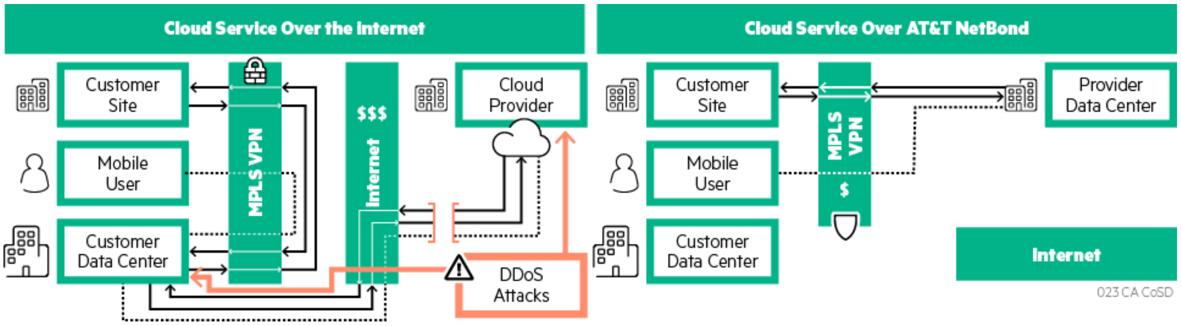
025 CA CoSD

Well-known cloud services partners that AT&T currently supports via NetBond.



022 CA CoSD

Security Benefits of AT&T NetBond



023 CA CoSD

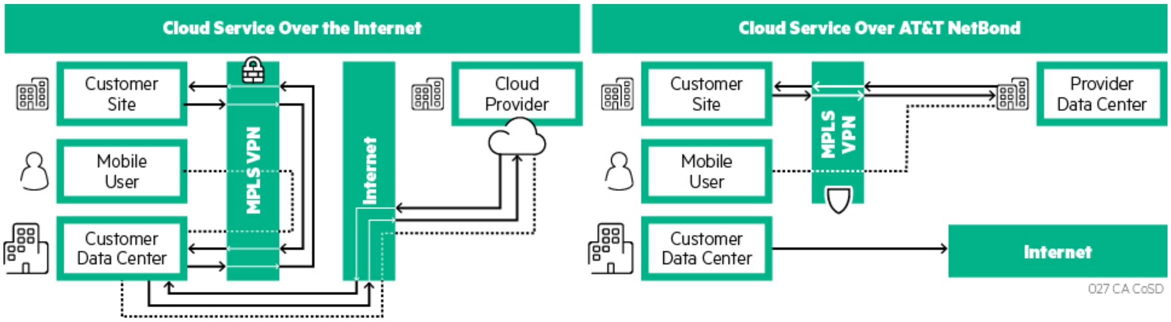
- Less secure, subject to Internet DDoS attacks
- Routing via Internet creates need for hairpin and VPN tunnel, adding expense and lowering performance
- Fragmented security policy and controls increase risks and cost

THREAT SUSCEPTIBLE

- MPLS segregates traffic from Internet threats
- MPLS VPN any-any routing increases performance and efficiency
- End-to-end security policy and controls minimize risk and cost

INHERENT NETWORK SECURITY

Performance Benefits of AT&T NetBond



- Inefficient; hair-pinning occurs when traffic is routed through additional locations to adhere to traffic security policies
- Public Internet relies on Best Effort data transmission based on congestion factors; critical data delivery is unpredictable

UNPREDICTABLE

- Direct routing of traffic to cloud: lower latency
- High performance and availability - low packet loss, jitter, and latency
- Full redundancy and failover provided via two carrier grade connection

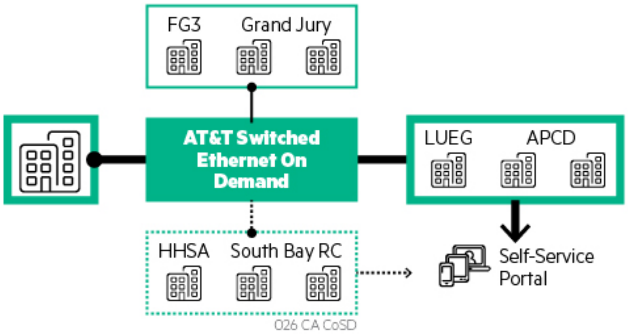
PREDICTABLE

Migration to AT&T Switched Ethernet with Network on Demand

Contractor's transformation plan for the County's wide area network (WAN) includes migration of all 115 OPT-E-MAN Metro Ethernet connected sites to the AT&T Switched Ethernet with Network on Demand (ASE w/NOD). Additionally, all data T1 sites shall be evaluated for migration and where available without significant special construction costs, sites shall be migrated to this new service. Special construction costs apply when fiber based transport is unavailable in the "last mile" from an underground or above ground exchange nearby a given site. The fiber install from these local exchanges is included in normal construction, but installing extended runs to new areas with no local exchange would be grounds for special construction. During the design and provisioning process, Contractor shall provide a list of T1 sites to the County with special construction costs for consideration. It is believed that 80-90% of the existing T1 sites are eligible for migration to this new service.

Using software defined networking (SDN) capabilities inherent to ASE w/NOD, bandwidth can be adjusted within 15 minutes from as low as 2 MB to as high as 1 GB. Coupled with real-time capacity management capabilities, this new service would allow rapid response to County bandwidth needs as well as enable the planning of additional throughput for scheduled events. Additionally, the deployment of fiber-based services would further improve consistency, availability, and performance of the remote sites across the network. The figure below lists benefits of AT&T Switched Ethernet On-Demand Service.

Figure 3. AT&T Switched Ethernet On-Demand Service Benefits



Fast Installation
Days in current fiber-enabled buildings

Dynamic Bandwidth
14 speeds with 5 CoS options

Flexible Deployment Models
Interconnect with existing AT&T Switched Ethernet; order services outside of current fiber footprint

Inter-LATA
Interconnect sites that reside in different cities and states

Digital Experience
Self-service portal to securely add and configure services

ASE w/ NoD Site Redundancy

Contractor has evaluated enabling additional remote site redundancy at key County facilities. The facilities listed below are historically some of the most important to County business functions and are the recommended sites for this enhanced service. It's important to note that the site list includes two sites that are currently on the Gigabit backbone (Sites 18 & 33), but are planned for migration to ASE w/ Network on Demand as a part of the Network Transformation, Backbone Consolidation project (see next section).

Site #	Site Name	Street Address	City	Zip Code
13	Children's Service Center (Adoptions Center)	6950 Levant St.	San Diego	92111
18	MTS Trolley Tower (Mills Building)	1255 Imperial Ave.	San Diego	92113
19	Lemon Grove District Office / FRC	7065 Broadway	Lemon Grove	91945
33	Health Services Complex	3851 Rosecrans St.	San Diego	92110
35	Animal Control-Central Shelter	5480 Gaines St.	San Diego	92110
55	Oceanside Service Center	1315 Union Plaza Ct.	Oceanside	92054
56	A. B & Jessie Polinsky Children's Center	9400 Ruffin Ct.	San Diego	92123
57	Child Welfare Services - Central	4990 Viewridge Ave.	San Diego	92123
80	Assessor/Recorder/Clerk Kearny Mesa	9225 Clairemont Mesa Blvd.	San Diego	92123
81	Assessor/Recorder/Clerk San Marcos	141 E. Carmel St., Bldg. 1	San Marcos	92078
95	HHSA FRC Center South Bay	401 Mile of Cars	National City	91950
190	HHSA FRC Center Escondido	649 W. Mission Ave.	Escondido	92025
205	Edgemoor Geriatric Hospital	655 Park Center Dr.	Santee	92071
260	Assessor's Revenue and Recovery	590 3rd Ave.	Chula Vista	91910
290	Access 211	8765 Fletcher Pkwy.	La Mesa	91942

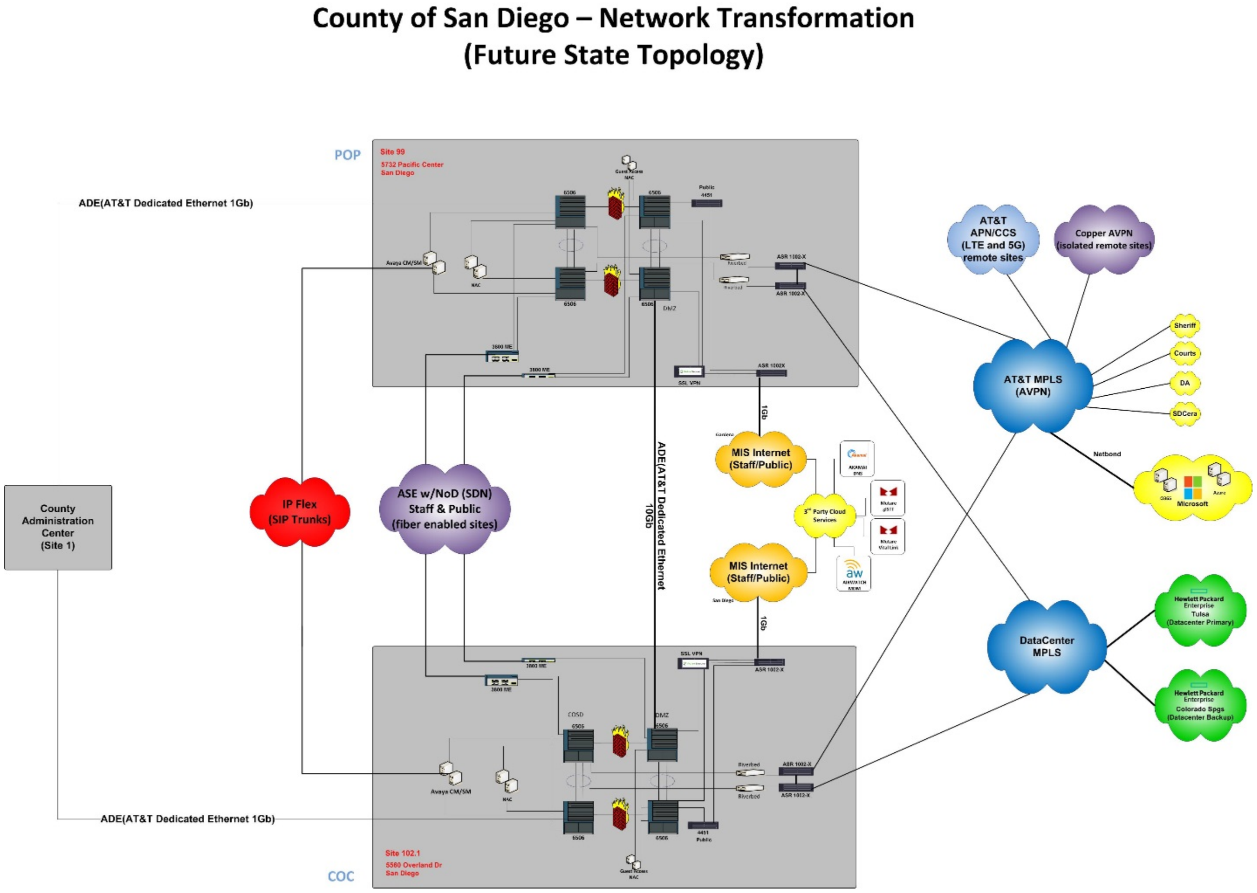
The standard Network on Demand design provides geo-redundant host circuits, however from the last Central Office, this diversity is reduced to a single fiber pathway to the remote site. The redundancy design involves provisioning a redundant circuit with diverse fiber path and infrastructure from an alternate central office. This secondary pathway extends to the remote site, entering via redundant entrance facilities. The circuits shall be ordered and built as stand-alone circuits and configured with minimal bandwidth, which leverages the Network on Demand near real time bandwidth provisioning capability to provide fully functional bandwidth in the event of a failure on the primary path.

Contractor shall provide the completion of requisite core transport design work which shall result in a per site construction cost for County consideration. This process shall also allow the County to evaluate cost of diverse entrance facilities. These one-time costs are responsibility of the County. The County may evaluate these costs and select sites that have the greatest benefit without being cost prohibitive. As these sites are selected, and one-time costs agreed, Contractor shall execute an order for the service. This offer shall remain valid over the first four (4) years of the contract term. County requests to add sites not previously listed shall be handled on a case by case basis.

Backbone Consolidation

AT&T also adheres to the concept of keeping it simple where possible. While some network solutions can be incredibly complex, the core architecture does not have to be. By reducing the number of core backbone sites (GigaMAN Connected), AT&T can simplify the network architecture while providing redundancy, sufficient bandwidth, and throughput for County business. This allows Contractor to right-size and tailor services in accordance with the needs of a location without the costs, equipment, and infrastructure inefficiencies that come with unnecessary capacity. The net result is standardization of transport connectivity across all County sites, providing the shortest path to services, in turn leading to predictable performance, improved security, reduced maintenance cost, and lower mean time to recovery (MTTR) in the event of an incident. The figure below illustrates the future-state network topology.

County of San Diego Network Transformation (Future State Topology)



Session Initiation Protocol (SIP) Core Expansion

Contractor’s network team has already begun the process of transformation within the County to phase out Time Division Multiplexing (TDMbased voice connectivity in favor of Session Initiation Protocol (SIP)-based solutions. Contractor’s SIP infrastructure is provided via two geo-redundant AT&T IP flex trunks that are dynamically available and sized to take a full production load of traffic in the event of a circuit failure. Currently, the SIP trunks are configured to support local outbound calling. Expanding on this foundation, Contractor plan to increase the capacity of these trunks to enable support of all Avaya core network controlled outbound calls, including local, long distance, and toll services. This expansion would eliminate outbound usage-based costs for these legacy resources units. Inbound calls would be migrated to SIP including Toll Free 800 services, which would substantially reduce the usage charges associated with Toll Free 800 services. Over the life of the Agreement, Contractor would continually evaluate the capabilities of these trunks to support additional voice and unified communication services.

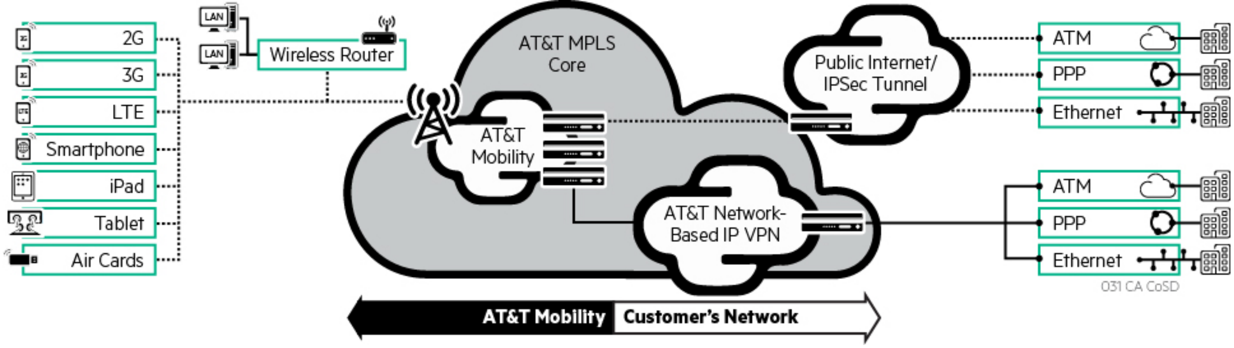
Future T1 Migration for Non-ASE with Network on Demand Sites

As identified earlier, T1 transport utilizing legacy TDM based connectivity, would be targeted for migration to ASE with NOD where possible. However, where fiber is not available without prohibitive construction cost, AT&T evaluates products such as copper-based AVPN that provides transport redundancy to the geo-redundant core. This service layers an AVPN service over a T1 copper circuit, providing AVPN cloud connectivity from a central office, creating pathway redundancy across the LAN. This solution continues to leverage the copper based wireline infrastructure that supports the site today, with a single point of failure still remaining on the “last mile” of transport to the remote site. As Contractor evaluates its options for eliminating T1 sites these factors may drive Contractor to pursue other alternatives.

Such an alternative could leverage the AT&T mobility network infrastructure using Commercial Connectivity Services (CCS) over a private Access Point Network (APN) service. Using LTE/4G (or potentially even 5G connectivity as it is brought to market), this service allows for secure connectivity through Contractor's mobility infrastructure, to connect back into the County network's AVPN edge at the County Operations Center and AT&T POP. While this solution eliminates the "last mile" single point of failure, early deployments using the LTE network would need testing to fully assess the impact of potential latency issues. As Contractor looks further down the industry roadmap, advancements promised in 5G connectivity have the potential of providing a high speed, low latency service that could meet enterprise requirements.

Through a collaborative evaluation of these options, Contractor, in conjunction with the County, would develop a roadmap to migrate all T1 based technology to connectivity options which are in line with Contractor's geo-redundant core infrastructure. The figure below illustrates this concept.

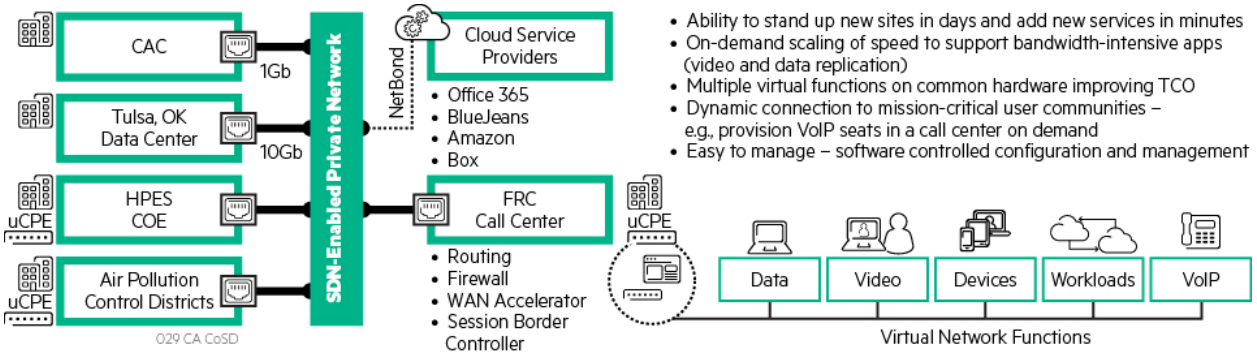
Commercial Connectivity Service – Enterprise Secure Connectivity using AT&T's LTE Mobile Network



Future Evolution of Software-Defined Networking-Based Services

During the life of the Agreement, AT&T would continually expand and improve its software-defined network (SDN) capabilities, where the local AT&T County network team would evaluate and recommend upgrades as they become viable and align with existing services. Midway through the Agreement term, Contractor anticipates key technical advances that could fundamentally affect the topology of the County network and the capital investment strategy. Building on the SDN foundation, new universal devices (Universal Customer Premises Equipment, or uCPE) could potentially represent a paradigm shift in how networks are provisioned and managed. Shifting capital cost to the provider, the County can take advantage of Network Function Virtualization, which provides services such as integrated LTE broadband backup, firewall, WAN optimization, and voice gateway functionality all on the same carrier managed device. Using Contractor's collaborative approach, Contractor would conduct production pilots, evaluate feasibility, determine business value, and make recommendations through the established Enterprise Architecture review process. The figure below illustrates the AT&T SDN enabled enterprise of the future.

AT&T SDN-Enabled Enterprise of the Future



- Ability to stand up new sites in days and add new services in minutes
- On-demand scaling of speed to support bandwidth-intensive apps (video and data replication)
- Multiple virtual functions on common hardware improving TCO
- Dynamic connection to mission-critical user communities – e.g., provision VoIP seats in a call center on demand
- Easy to manage – software controlled configuration and management

As the needs of the County continue to evolve, Contractor would continue to collaborate with business unit and CTO staff and Contractor's cross-framework partners to understand the challenges and develop best-in-class solutions. Contractor believes that transformation is an iterative process, requiring strategic planning and vision coupled with practical approaches that ultimately make certain that functionality is provided to the customer in the most expedient way possible. Technologies identified in this solution are just the beginning of a contract lifecycle of change, but would provide a foundation for growth as Contractor moves forward as a trusted advisor to the County.

- Deployment plan for resources and use of facilities

The local, dedicated AT&T team—fully embedded in the solution lifecycle—provides all design, implementation, support, and monitoring of transformation activities. Technical personnel assigned to the County of San Diego and dedicated to the program are located at Contractor's Trade Street facility to maintain a fairly central base from which to service the County. All solutions leverage the AT&T Internet Data Center (IDC) in San Diego County as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. Working from the local Trade Street facility, Contractor's SMEs would monitor, support, and maintain the remote services.

- Key methodologies and processes in solution

The local, dedicated AT&T team views transformation as an ongoing activity. By constantly monitoring what is currently available technology as well as keeping abreast emerging technology, Contractor is able to deliver concepts and ideas for consideration by the CTO. Contractor has already begun the task of installing ASE w/NOD at all new County sites; this task was preceded by the installation of two new host circuits, one each at the point of presence (POP) and County Operations Center (COC). Contractor would leverage this existing infrastructure as Contractor begins migration to ASE from the existing OPT-E-MAN connected county sites, with Contractor's project management staff coordinating the implementation(s). Work is also currently underway to consolidate the core GigaMAN backbone sites, with high-level architecture design already underway. The expectation is that the first two sites would be transitioned by approximately the end of the year.

Discussions with the County have already begun and are continuing related to cloud providers and the benefits that NetBond can provide. AT&T remains dedicated, so when and if the County decides this service is necessary—based on migration of various components to cloud providers and infrastructure—the local, dedicated AT&T team would bring in any resources needed to facilitate the entire process. This process would span final design and associated documentation, ordering of infrastructure components like circuits, and coordination with AT&T core services as well as cloud providers to provide a seamless transition. The local, dedicated AT&T team would continue to leverage all resources available within Contractor's local organizations (Engineering, Project Management, and Architecture) to provide all aspects of transition and transformation activities.

- Automated systems and tools involved in solution

The local, dedicated AT&T team uses a myriad of tools and automated systems to perform implementations and support operations and performance. These tools include Cisco Prime Infrastructure, the CA Spectrum suite, SNTC (Smart Net Total Care), Riverbed Cascade, and Panorama. Cisco Prime Infrastructure is used to centrally manage configuration as well as gather data related to changes, performance, inventory, and licensing. The CA Spectrum suite—which includes Spectrum and E-health—is used to monitor availability, performance, and inventory management; it also provides trending and analysis for traffic utilization. SNTC is a Cisco product used to manage support services as well as automate the process of gathering data for direct vendor support in the event of a problem. Riverbed Cascade is a deep packet analysis tool that uses NetFlow data, which is gathered passively and directed to it in an automated manner as well as active packet capture and analysis. Finally, Panorama is a Palo Alto Networks product that provides a central repository for logging, inventory of the Palo Alto components, licensing management, software image management, and analysis capability for the County security infrastructure.

Voice Services Transformation Project

- – Description of solution to meet the requirements

The solutions highlighted in this section include transformation initiatives planned for implementation early in the term as well evolutionary technologies that may arise later in the Agreement life cycle. Relative to statements focused on technology not yet available for deployment, AT&T would roadmap and evaluate the feasibility of these solutions during the Agreement life cycle. If identified as a viable replacement to existing services, AT&T would make recommendations for upgrades in line with refresh obligations or as otherwise agreed with the County.

AT&T's approach to transforming voice services focuses on enabling new features and capabilities used by both the End-Users and County constituents built on a foundation that is redundant, resilient, and highly available. The ultimate goal in developing the next architecture for voice services is to harden the core and edge locations and to offer robust and feature-rich UC for each and every End-User of enterprise voice services.

Core Network Transformation

Transformation activities at the Avaya Voice Core would migrate from any remaining traditional PBX architecture and provide an infrastructure reduction resulting in lower power consumption and reduced trouble tickets while minimizing disruption to users. This approach provides migration from the existing G650 Port carriers or other gateways, and upgrades them to G450 or G430 gateways. This transition would eliminate legacy IP Server Interface (IPSI) boards, mitigating risk by replacing end-of-life equipment and reducing the physical footprint in the data centers. This transition would take place at the Point of Presence POP as well as the County Operations Center (COC). In addition, the "TN" modules would be replaced with Media Modules in the G450s or G430s, and the digital signal processor (DSP) resources would be replaced with local media resources at the gateway as well as in the Avaya media servers.

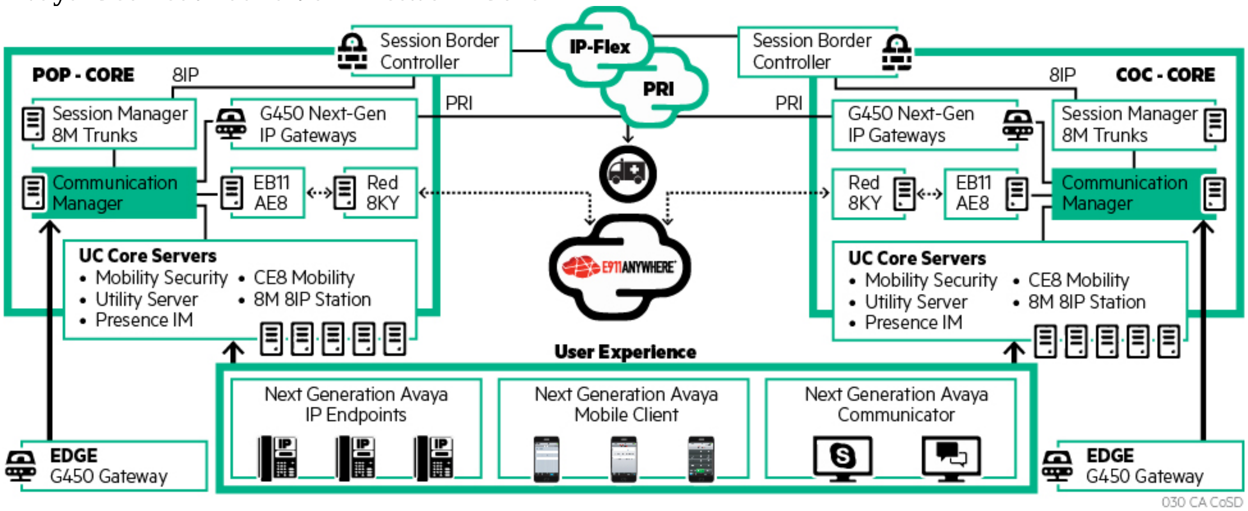
This highly available architecture would provide seamless failover between the COC and POP, with no single point of failure of the Core VoIP gateways. The architecture not only would provide centralized management between the two "Core" locations—POP and COC—but would also provide access to the remote locations, or locally survivable processor (LSP) sites.

Additional implementations would take place at the Core that would serve as the foundation for offering new and enhanced UC capabilities for End-Users, such as external mobile SIP endpoints on County- managed devices. This would be made possible by the Avaya Client Enablement Server as well as the Avaya Presence service for telephony presence on a mobile device.

Geo-redundant Voicemail

Contractor's solution includes the advancement and transformation of enterprise voicemail services, which replace the current, single-site-based voice messaging platform located at the AT&T POP, with a fault-tolerant, geo-redundant voice messaging platform located at the AT&T POP and COC. The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations. This geo-redundant design incorporates live replication of the voicemail database, messages, and greetings between the AVST Call Servers at the AT&T POP and County Operations Center using AVST's never fail technology. The following figure illustrates the Avaya Geo-redundant VoIP Network Core. This solution is expected to be in place as the next agreement is signed. Using a roadmap strategy, AT&T Centrex users would be migrated over time to this platform, as specified below in the paragraph highlighting AT&T's Centrex migration roadmap.

Avaya Geo-redundant VoIP Network Core



POP - CORE
8IP
Session Border Controller
IP-Flex
PRI
Session Border Controller
8IP
COC - CORE
PRI
PRI
Session Manager 8M Trunks
G450 Next-Gen IP Gateways
G450 Next-Gen IP Gateways
Session Manager 8M Trunks
Communication Manager
EB11 AE8
Red 8KY
Red 8KY
EB11 AE8
Communication Manager
UC Core Servers
• Mobility Security • CE8 Mobility
• Utility Server • 8M 8IP Station
• Presence IM
E911ANYWHERE
UC Core Servers
• Mobility Security • CE8 Mobility
• Utility Server • 8M 8IP Station
• Presence IM
User Experience
Next Generation Avaya IP Endpoints
Next Generation Avaya Mobile Client
Next Generation Avaya Communicator
EDGE G450 Gateway
EDGE G450 Gateway
030 CA CoSD

The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations.

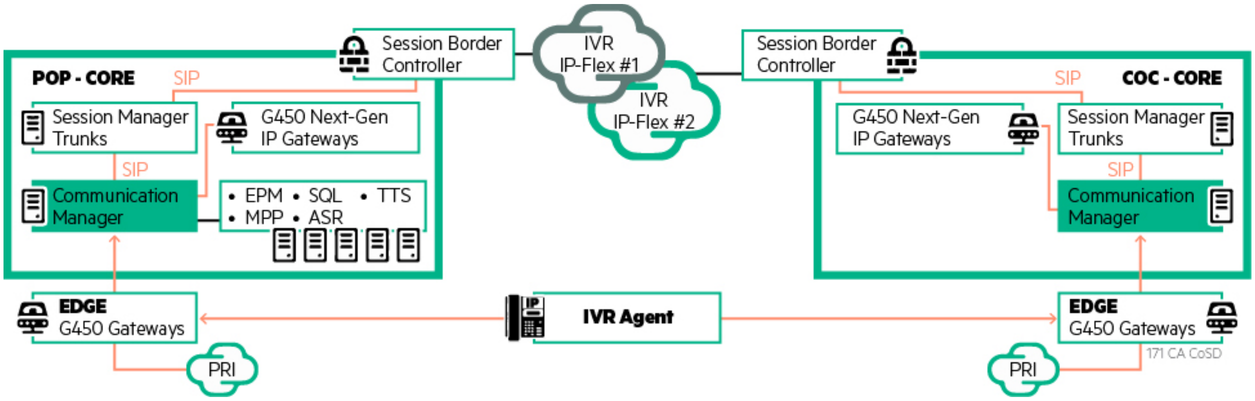
Interactive Voice Response (IVR) Transformation

Lastly, AT&T's transformation plan for Voice Services extends to Core adjunct services, such as its Interactive Voice Response (IVR) solution. The County's IVR infrastructure is built around the Avaya experience portal, which is a high availability contact center solution located at the AT&T POP. This platform provides access for external constituent service to County departments (such as Animal Services, Land Use Environmental Group, and various departments within the Health Human Services Agency) using features such as IVR, self-service, touch-tone, and speech recognition services. This scalable, high availability infrastructure provides many options for programming and agent integration, allowing customization for any type of constituent-facing contact center service.

The platform would undergo near term changes to external telephony connectivity as AT&T initiates plans to implement dedicated, fault tolerant inbound and outbound IP flex SIP trunks for the County's IVR infrastructure at the AT&T POP and County Operation Center. This change would prevent the Core IVR solution from impacting enterprise voice traffic, allowing business units to conduct high volume contact center activities such as outbound dialing campaigns. This new capability would provide a more standardized RU that business units can use to leverage the platform in meeting their business needs.

Over the term of the Agreement, AT&T would focus on roadmap initiatives and develop proposals to increase redundancy and resiliency of Core IVR applications as well as provide additional feature benefits such as automated agent call back and web chat.

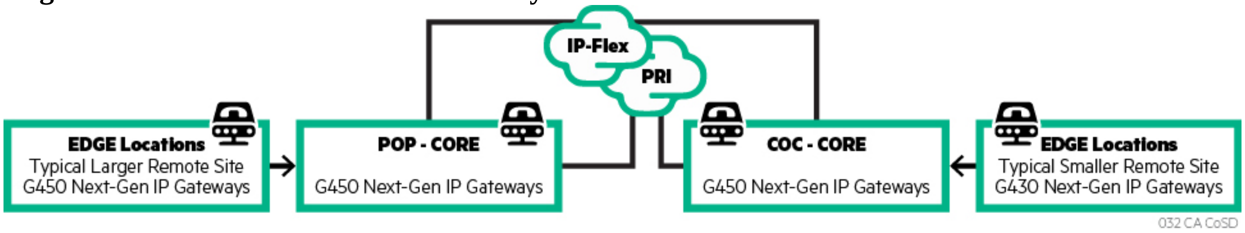
Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.



Edge Network Transformation

At the remote Edge, AT&T would replace all legacy cabinets and gateways (G650, MCC, SCC, CMC, and G700 series) with the latest generation of G450 or G430 gateways, providing LSP for resiliency. In the County, 81 sites have been identified as needing remote edge transformation to accommodate the implementation of VoIP phones. These 81 locations currently have digital telephones served from legacy cabinets and gateways. The Avaya G450 Media Gateway is a multi-purpose media gateway. The figure below**Error! Reference source not found.** illustrates Edge or Remote Site Network Connectivity. It works in conjunction with Avaya Communication Manager IP telephony software running on Avaya S8XXX Servers to help deliver intelligent communications to enterprises of all sizes. The G450 combines telephone exchange and data networking by providing public switched telephone network (PSTN) toll bypass and routing data and VoIP traffic over the WAN. The G450 features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. The G450 provides full support for Avaya IP and digital telephones as well as analog devices such as modems, fax machines, and telephones. Telephone services on a G450 are controlled by an Avaya S8XXX Server operating either as an External Call Controller (ECC) or as an Internal Call Controller (ICC). The G450 supports the Avaya S8300 Server as an ICC or, when the S8300 is installed in another media gateway, as an ECC. An ICC would be installed and used as a LSP. This is designed to take over call control in the event the ECC fails or the WAN link between the branch office and main location breaks. The LSP provides full-featured telephone service survivability for the branch office. The G450 itself also features Standard Local Survivability (SLS), which provides basic telephone services in the event that the connection with the primary ECC is lost.

Edge or Remote Site Network Connectivity


IP-Flex
PRI
EDGE Locations
Typical Larger Remote Site
G450 Next-Gen IP Gateways
POP - CORE
G450 Next-Gen IP Gateways
COC - CORE
G450 Next-Gen IP Gateways
EDGE Locations
Typical Smaller Remote Site
G430 Next-Gen IP Gateways
032 CA CoSD

Centrex Migration

As detailed in the Voice Services section, the majority of voice services for the County are provided by the Avaya enterprise voice network. A small subset of the County's office sites does have voice services delivered by AT&T's Centrex business telephone service. Centrex service is typically deployed to smaller County sites that contain 1-20 users. At present, there are roughly 117 sites with Centrex voice services. While the AT&T Centrex business telephone services provide stable telephony and voicemail services, these locations are separated from the remainder of the County's End-User population and are not able to take advantage of the full UC capabilities offered to Avaya enterprise users. With this in mind, the need to transform the features and capabilities for current Centrex voice services locations and to enable the users with the ability to use Avaya enterprise voice feature is a business priority. AT&T has developed a transformation approach to migrate a majority of these users' stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed during the term of the agreement.

The migration of Centrex users would begin with the deployment of stand-alone IP-based telephones at sites with existing data network functionality. This solution would provide services for VoIP telephone sets that is centrally managed by the Avaya geo-redundant voice cores at the AT&T POP and County Operations Center. While these sites would not have local survivable gateways, they would take advantage of the data network for their connectivity to the enterprise voice infrastructure. Of the roughly 117 Centrex sites across the County, 80 of these locations would be eligible for this service. Through this migration, over 65% of the Centrex remote sites and more than 272 individual stations would be converted to the Avaya enterprise standard. These sites/users would be provided new centralized voicemail and UC functionality as well as a new telephone set that leverages the County's investment in the data network for connectivity.

A greater challenge in the elimination of the legacy Centrex solution is associated with locations that do not have data network access. These locations are typically very small and remote locations that only require simple telephone service for communication. The migration of these services would be the topic of transformative roadmap planning during the term of the Agreement. Currently, AT&T is developing a Centrex replacement technology that is expected to provide transport and service options that would be evaluated for transformation. Some additional possibilities include the use of the mobility network for connectivity to the enterprise infrastructure, using an emerging technology called voice over LTE (Long Term Evolution).

Additionally, there are some remaining Centrex stations that have been placed throughout the County in locations with data network services where off-net phones are provided as a business requirement, such as elevator phones and emergency lines (red phones). As the Centrex replacement solutions mature, these solutions would also be evaluated for migration to a similar, off-network service so as to maintain the redundancy required for the specific use case.

VoIP Telephone Standard

The End-User experience is the single greatest change that would affect the County users in the proposed voice transformation. While the voice network is continually upgraded at the core, many telephone sets across the County have remained unchanged in over 15 years. By moving to new VoIP telephone sets, the County users would enjoy the benefits of a new device, along with improved reliability and performance.

There is significant value in resiliency that IP telephones offer over legacy TDM telephones. TDM devices require a dedicated port with a dedicated wire to connect to a local gateway. There are many points of potential failure, including the wire, gateway card, gateway power supply, gateway processor, and so forth. An IP telephone connects universally to any network port to facilitate registration to one of several points of call processing. An IP telephone would primarily be registered to the Session Manager Registrar at the core; there is a Session Manager Registrar at both core sites for high availability. In the event an edge location becomes fragmented from the WAN, the IP telephone would register locally to the G450 gateway with a local survivable processor (LSP).

Avaya/Skype for Business Integration

Another important pairing with a VoIP deployment is the implementation of E911 services. E911 allows for a continually managed registry of location data for each workstation so first responders have necessary information to effectively respond to an emergency call.

Another key End-User benefit associated with the Voice Transformation initiative is the integration of the Avaya enterprise voice system with Microsoft Lync (Skype for Business client). Using available licensing and open Application Programming Interfaces (API's), **Avaya Communicator** extends Avaya Aura real-time collaboration capabilities to Microsoft Lync 2010, 2013, or Skype for Business 2015, 2016 clients to provide users with a unified, consistent collaboration experience from their preferred applications and devices. The Avaya Communicator for Microsoft Lync service adds functionality to Microsoft Lync clients using only the Lync/Skype for Business standard client access license (CAL). Features include telephony presence aggregated with Lync's machine and calendar presence through Lync/Skype for Business client API and Lync/Skype for Business IM and desktop sharing, click-to-call control of PBX desk phones, voice and video, enterprise dial-plan support, toast pop-ups enabling incoming calls to be answered, and Reply with IM as well as a conversation window pop-up to access Avaya mid-call features and the ability through the Share My Bridge feature to launch a conference call and or collaboration session from within the client.

Avaya Collaboration Services

Avaya Collaboration Services interworks on the End-User PC with Communicator for Lync to provide UC services originated from Microsoft Office Suite, Outlook, SharePoint, and Internet Explorer as well as Mozilla Firefox and Google Chrome browsers.

When in Outlook or SharePoint, hovering over an End-User's name or presence indicator presents their contact details. The End-User now has the opportunity to IM, email, make a voice or video call, or schedule a meeting with this End-User. The End-User's presence is also displayed.

In addition, Collaboration Services would detect a number embedded in an email or a Word, Excel, PowerPoint, or SharePoint document and allow calls to be made to this number through Communicator for Lync. As with a call originated through the Lync/ Skype for Business End-User interface, a conversation window would be presented to provide the End-User with call control options for the duration of the call.

Collaboration Services automates the process of Join or Host a conference call. With this feature, the End-User can launch a conference call and/or a web collaboration session. The Collaboration Services would determine whether the End-User is the Host or a Participant to this call and uses the appropriate access passwords to access this call.

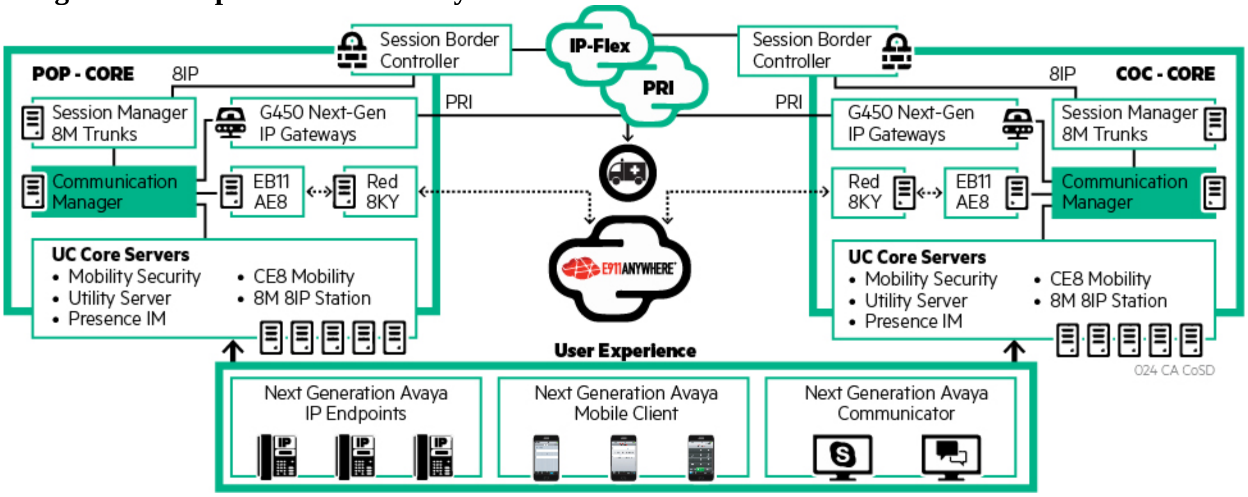
Collaboration Services, when used with Internet Explorer, Mozilla Firefox, and Google Chrome browsers, would recognize number patterns on web pages, and through the use of an intelligent algorithm applies enterprise, national, and/or international dialing rules to highlight these as phone numbers. These phone numbers can be dialed from a web site using the Avaya Communicator for Lync.

If a phone number is on an enterprise web page, Collaboration Services would take this number, access Active Directory, and pull down additional information for this End-User. This information is displayed on a contact card. The contact card is also populated with icons that enable the End-User to send an IM and see the presence of this contact, make a voice or video call to the contact, and schedule a meeting.

Integrated Enterprise Mobility

A final End-User benefit of the Voice Transformation initiative is integration of the End-User's voice and UC capabilities with their mobile device. Integrated Enterprise Mobility brings seamless interoperability with the desktop and desk phone. The figure below illustrates components of the County Integrated Enterprise experience.

Integrated Enterprise for the County



Integrated Enterprise Mobility brings seamless interoperability with the desktop and desk phone.

Features that span the desktop and desk phone are extended to the mobile End-User and are transparent in functionality. Examples include the following:

- Start a call from the County's desk (either desktop client or desk phone) and, if the County chooses to become mobile, simply select a button on the mobile app to move the call from the original location to the mobile device.
- Call processing from a mobile device extends a robust feature set (Hold, Transfer, Conference, Speaker, Mute, etc.) to the End-User so that transitioning from desktop or desk phone is seamless. The End-User experience is the same.
- The UC features of Avaya Communicator include visual voice mail to filter and sort voice messages. Use the visual voice mail feature to respond to important messages quickly. Communication History logs help the County traces the history of the County's enterprise calls and voice messages. Use Avaya Communicator to increase the productivity of the County's enterprise with tools that enhance collaboration, improve responsiveness, and lower costs for IT and End-User support.

- Deployment plan for resources and use of facilities

The local, dedicated team provides all the design, implementation, support, and monitoring of transformation activities and is fully embedded in the solution life cycle. Technical personnel assigned to the County are dedicated to the program and located at Contractor's Trade Street location, maintaining a central location from which to service the County. Additional leveraged resources may be engaged to support transformation and would operate under the direction of the local team.

All solutions use the AT&T POP as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. All County facilities with voice network connectivity would house infrastructure and telephone sets necessary to provide service.

Key methodologies and processes in solution

The dedicated LCM team is embedded in the full life cycle of every enterprise voice and UC solution—from the initial gathering of requirements, through the design and implementation phases, to managing and monitoring, and even decommissioning when requested. Through customer meetings and service reviews, the team creates the proper solution that is chosen and sized appropriately.

Contractor would use standard Project Management methodologies in the scoping and execution of any new installation. AT&T architects and engineers would also use approved processes in their design and equipment placement activities. Enterprise voice and UC options are continually evaluated based on County business requirements in addition to current and emerging technologies.

Contractor's technical enterprise architecture team evaluates new products and standards to make recommendations to the CTO. When a recommendation is approved, Contractor's team moves forward with implementation recommendations including refresh of existing equipment and rollout schedules. For equipment issues, Contractor's Service Desk and engineering team work to identify and remediate the problem.

- Automated systems and tools involved in solution

To support quality voice service within the support levels defined by the new agreement, Contractor's subject matter experts (SMEs) use numerous automated tools. These tools enable Contractor to continuously monitor the overall health and performance of voice appliances, provide tools to assist in rapid restoration through fault isolation, and perform traffic analysis, as discussed below.

Contractor delivers complete manufacturer system maintenance coverage on all County Core Voice Services assets. The Avaya maintenance services include Avaya Expert Systems and Secure Access Link. Avaya Expert Systems provides the County Core Voice Services a maintenance database of more than 30,000 Artificial Intelligence Algorithms (AIAs) with scripted automation that is able to automatically correct many known system and software-related issues. Avaya Secure Access Link (SAL) is a centralized consolidation point for all Avaya Core systems for health and alarming monitoring, secure remote access using secure outbound-only HTTPS standards, and an integration point for Avaya Expert Systems. Together, these tools provide the County's Avaya Core Voice Services complete health monitoring and rapid issue resolution. Avaya Expert Systems and Secure Access Link are online and engaged 24/7 to diagnose and attempt to resolve known system alarms, clear many service-affecting issues, and escalate to engineering resources for prompt attention when necessary to allow service restoration or outage avoidance to County users.

Contractor's Voice Services team uses Nectar's Unified Communication Management Platform (UCMP) and leverages its complete suite of innovative features to provide the County enhanced integrated UC network services. Nectar provides multi-vendor management services including application dependency tree visual alerting and vendor knowledge modules, which assist Contractor's SMEs to proactively pinpoint and resolve cross-platform integrations issues to quickly restore services to County users. The UCMP also includes real-time network quality-of-service reporting using RTP (Real-time Transport Protocol) Control Protocol (RTCP) integration and can provide Contractor's team with the capability to create simulated traffic injection between designated network segments for analysis. This enables SMEs to monitor and report on all VoIP-related traffic transmissions. The quality-of-service reporting tool provides per-hop statistics, and in many cases assists in quickly identifying improper packet handling hop points, driving efficient resolution of network quality-of-service issues. The Nectar platform includes statistical resource utilization data gathering and storage that enables trending analysis and capacity planning so County users are not impacted by growing resource needs. Finally, all these capabilities are wrapped into an intuitive and customizable dashboard for use with visual and electronic alerting from sophisticated threshold configurations that drive the ability to acknowledge, respond to, and correct issues proactively in many cases before County users are aware of or report an issue.

E911 Manager would automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T MPLS network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 911 call routing service that can connect a 911 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

Storage Architecture Transformation Project

- Key Considerations and Potential Alternative Approaches

Architect Storage to Embrace Tiers of Well-Defined Storage: The solution being implemented by Contractor during the data center consolidation architects the design to embrace tiers of well-defined storage. The key considerations that went into the storage solution include cost and the ability to meet the County's requirement to keep the storage infrastructure current by refreshing storage components every 5 years. Contractor also considered the storage growth requirements and developed a solution with 20% year-over-year growth projected for the first 5 years.

In addition to Contractor's solution, which builds on the storage that is in place for the County on completion of the transition activities, Contractor considered two alternatives:

Storage Tiering Alternative: Contractor considered providing a 3PAR 20000 with 15,000 RPM drives and/or SSD as Tier 1, 10,000 RPM drives as Tier 2, and 7,200 RPM drives as the archive tier. This would provide a clearer delineation of the tiers from a performance perspective but would have resulted in a higher total storage cost than Contractor's actual solution. Contractor would continually monitor the performance of the storage environment.

Shared Storage Alternative: The second alternative is to provide storage as a leveraged service. This approach is similar to cloud storage in that the storage infrastructure would be shared with other non-County of San Diego clients, but the storage volumes would be dedicated to the County of San Diego. There would be no co-mingling of data on storage volumes, but the underlying storage hardware would be shared. All storage volumes would be securely wiped after they are no longer needed by the County, to prevent any chance of the County's data being exposed to non-County of San Diego customers on the leveraged storage infrastructure. This solution provides a lower cost per GB of storage. Using leveraged storage, Contractor could also provide the required tiers of storage using either the recommended solution or the Storing Tiering Alternative. However, with this leveraged approach, the County would not be able to specify the hardware refresh to meet their desired schedule, so Contractor rejected this solution.

- Description of solution to meet the requirements

Solution Summary: Upon completion of the data center consolidation, the storage architecture shall comprise a dedicated storage area network (SAN) with a 3PAR 20000 storage array in Tulsa providing tier 1, 2, and archive storage to all data center servers, consolidated in Tulsa. End-User data storage shall be provided directly from the new network-attached storage (NAS)-capable 3PAR. Otherwise, End-User data storage shall be the same. All 3PAR data shall be backed up locally using HPE Data Protector with a StoreOnce Virtual Tape Library (VTL) as the backup target. All backup data and disaster recovery (DR)-required 3PAR data shall be replicated to the DR site in Colorado Springs. The data center solution shall include immutable storage, which would also be replicated to the DR site. For the San Diego sites, backup data shall be replicated to the DR site instead of being copied to tapes, for remote offsite storage. Finally, the immutable storage refresh and reconfiguration shall be a newer version of the same immutable storage.

The Contractor's storage architecture following transition includes updated storage equipment, which shall be refreshed on a 5-year cycle. The storage array technology is flexible and efficient, designed to keep pace with the County's requirements as they evolve. Tiers 1 and 2 have been redefined to reduce cost without sacrificing performance. The backup solution would consolidate all of the County's backup needs into one capacity-driven solution that eliminates physical tapes from the environment. The location of the immutable storage solution would change with the Data Center Consolidation, and the hardware would be refreshed.

Contractor would continually evaluate the various storage tiers used by the County as their storage requirements evolve, with an eye toward providing the right storage solution for each tier. However, the storage solution that would be in place following Transition provides ample opportunity for growth in terms of storage and performance, and achieve tier storage service is based on 3PAR 20000 storage devices—the latest innovation in 3PAR enterprise storage from HPE.

Contractor would continually evaluate the County's storage archiving needs and consider a cloud-based archive storage solution if/when cloud-based archiving meets the County's approval.

Rationale: The solution Contractor provides meets the County's post transition requirements and would allow the County to transform its storage architecture over time, as needed. The 3PAR is capable of supporting 15 PB of usable storage capacity. It would support a range of disk drive technologies from 7,200 RMP, 10,000 RPM, and 15,000 RPM Serial Attached SCSI (SAS) drives and solid state disk drives (SSD). The 3PAR supports storage migration without interruption via 3PAR-enabled storage peer motion (SPM). The 3PAR supports the following:

- Thin provisioning (TP), which is a method of optimizing the efficiency with which the available space is used in SANs. TP operates by allocating disk storage space in a flexible manner among multiple users, based on the minimum space required by each End-User at any given time.
- Auto tiering is a real-time intelligent mechanism that continuously positions data on the appropriate class of storage based on how frequently the data is accessed. This improves application performance.
- Compression, which reduces the number of bits needed to store or transmit data.
- Data deduplication, which reduces storage needs by eliminating redundant data. Only one unique instance of the data is actually retained on storage media.
- Federal Information Processing Standard (FIPS) 140-2—data at rest encryption to protect against loss or theft.
- Industry standard redundant array of independent disks (RAID) configurations to meet disk fault tolerance requirements and optimize performance.
- Remote and local replication for future refresh migrations on live data (meaning no down time required).
- Quality of Service to make certain bandwidth is available when needed.

The immutable storage solution has the capacity to support future growth in data storage requirements. The County's Document Processing Center (DPC) storage, which also uses 3PAR, would allow the DPC storage to evolve as needed. The direct attached storage would remain the same, and Contractor would continually evaluate services that use direct attached storage and work with the County to determine when/if those services can be migrated to SAN and/or cloud storage.

Timing: Contractor performs weekly reviews to assess capacity usage and determine whether changes are needed, taking into account any anticipated changes from the County.

Risk Considerations: This approach poses minimal risk based on continued use of the same platform. All capabilities are currently available, and the County can take advantage of this on a schedule that meets its needs.

- Deployment plan for resources and use of facilities

The Contractor's Storage Administration team would perform the assessments on an ongoing basis, as described above.

Storage hardware would be located in the Tulsa data center and at the San Diego sites, which include the DPCs at Lemon Grove and Viewridge. The storage would be replicated to the DR site in Colorado Springs.

- Key methodologies and processes in solution

At the 5-year refresh cycle, Contractor would continue to use replication extensively. Contractor's storage administration staff is well versed in array-based replication capabilities and would be able to extend replication to include the new hardware with little to no disruption to the County's compute services.

- Automated systems and tools involved in solution

Enterprise storage (3PAR) has native replication capabilities built in and enabled by the storage array software. The primary tool used to accomplish the storage transformation would be SPM. This type of replication is automated and keeps storage in sync on both copies of the data.

- Key Considerations and Potential Alternative Approaches

Classify County data and assign it to the appropriate tier: When evaluating solutions to classify County data, Contractor took the following items into consideration:

- The significant volume of the County's unstructured data currently stored in file shares, SharePoint, Exchange, and a range of other repositories; however, not all unstructured data is to be treated the same way.
- It is important to be able to classify data based on its importance, sensitivity, and need for access.
- By classifying unstructured data, Contractor can automatically direct it to appropriate data tiers to reduce storage costs while providing the County with the appropriate access requirements.

This initiative, is a primarily technology-driven effort coupled with consulting services to guide configuration of the solution. The alternative approaches are tied to specific implementation models for the various product suites that could be used to deliver this auto-classification.

- Description of solution to meet the requirements

Currently, a wide range of products is available to support the automatic classification of unstructured data/content. Through the application of policy enforcement, content can be targeted to different tiers of storage. The County has assessed a range of these products and has found several that appear to meet the requirements. Contractor would work with the County to design, configure, and implement the selected product suite.

Contractor would recommend, however, the County implement HPE's ControlPoint software. HPE is recognized by Gartner as a leader in Information Governance and Information Management (IM/IG). ControlPoint provides a robust platform for identifying, analyzing, and managing diverse types of information stored in enterprise repositories. Through continuous monitoring of enterprise repositories, ControlPoint can classify unstructured data based on a range of County identified metadata, including standard classification structure of Public, Sensitive, and Confidential documents, applying policy to facilitate optimal storage strategy.

Rationale: Applying file management tools would help the County to reduce its information footprint by identifying redundant, obsolete, and trivial (ROT) data; this can lead to reduced storage costs.

- Redundant data consists of duplicates such as unauthorized copies of documents, emails, records, or database information residing in file shares, SharePoint sites, mail systems, and databases.
- Obsolete data consists of information that is no longer in use or is out of date. Determining whether data is obsolete can be based on its creation date, last modified date, or access date; then assess this information in conjunction with an appropriate retention policy.
- Trivial data is determined by file type, where the file type has no content value, such as executables, system files, and thumbnails.

Additionally, such a solution can be used to tag and classify unstructured data, and through automatic application of policy, data can be targeted to specific tiers of storage or even deleted if appropriate. Ultimately this would lower the total cost of storage.

Timing: After completion of transition, Contractor recommends approaching unstructured data classification on an enterprise scale. Contractor's approach begins with an assessment and a pilot of a limited set of data/ repositories, while building out the required solution architecture to support the County's entire unstructured data environment. Contractor's solution includes resources to manage the indexing of the remaining data, keep indexing up to date throughout the Agreement, and cross-train others on the support team.

Risk Considerations: Given the volume of data currently stored by the County, an enterprise-wide implementation can expose significant risk. Contractor mitigates the potential risk by starting the project with an early assessment to help define and test the County's data categories. Following the Milestones presented below also mitigates this risk through careful planning and testing prior to enterprise-wide rollout.

Key Dependencies: This solution is dependent on the availability of tiered storage architecture and file management/auto-classification platform, whether ControlPoint or an alternative selected by the County.

Milestones: Key Milestones for the data classification project include the following:

- **Milestone 1 – Develop Data Categories** – Building on the County's existing set of categories such as security classifications—Public, Sensitive, or Confidential—Contractor would use automated tools and common categories to develop a set of categories specific to the County. These categories could include County Groups, Function, and Availability. Contractor would select a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of theses draft categories would not affect documents in production systems.
- **Milestone 2 – Refine and Test** – This step helps to determine the relevance of the categories to enterprise documents. Refining a category is done by adjusting the weighting of a term or the selection threshold, or by adding field text. These activities can be done individually or in combination. A category can be published, making it available for use in automatic policy execution against content managed by the tool suite.
- **Milestone 3 – Auto-Classification** – Once County data is categorized; Contractor applies policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, Contractor can automate policy application, governing all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating data across repositories helps to minimize storage costs and reduce discovery times.
- **Milestone 4 – Knowledge Transfer** – Following the pilot effort, further described below as part of Contractor's methodology and key processes, and validation of results, Contractor's subject matter experts (SMEs) would conduct knowledge transfer to the support team for the County to maintain the system and to index all County unstructured data.
- **Milestone 5 – County-wide Rollout**

- Deployment plan for resources and use of facilities

Contractor would initially provide a team of SMEs to guide the planning and piloting efforts. This team would work onsite, collaborating with the County's staff and the support team to define requirements and validate the results of the project. This team would also conduct knowledge transfer to facilitate extending the implementation and support County-wide. Contractor SMEs would remain available as required to provide reachback support. The infrastructure for the product of choice would be installed in the Tulsa Data Center.

- Key methodologies and processes in solution

A data classification project begins by working collaboratively with the County to gain insight and understanding of the legacy data landscape. This helps Contractor to define the benefits of a full legacy data cleanup solution, create a Solution Roadmap illustrating the go-forward plan, and implement the auto-classification solution infrastructure. Contractor then conducts a pilot, where Contractor would sample approximately 1 TB of data currently residing on the County's existing file share environments to determine appropriate classification structure and to demonstrate how data can be targeted automatically to different tiers of storage based on the classification. Additionally, the assessment would showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made regarding data management, archiving, retention, and retirement. Following the pilot, Contractor SMEs would perform knowledge transfer to the Contractor account team to facilitate indexing of the remaining data and then applying the solution to provide ongoing auto-classification of unstructured data.

- Automated systems and tools involved in solution

Contractor would use ControlPoint software or an alternative platform selected by the County to auto-classify unstructured data.

- Key Considerations and Potential Alternative Approaches

Develop Archival Solutions for Portfolio Applications: The County has more than 400 applications currently supporting its departments and citizens. These applications rely on different types of data—some unstructured, such as document management and SharePoint oriented data—and some with structured data. It is important to consider and evaluate the full portfolio of applications to determine the appropriateness of data archiving to reduce the data footprint and storage costs. There are two potential alternative approaches:

- **Approach 1:** Conduct an enterprise-wide assessment to determine the applications that are to be targeted for data archiving. Based on this assessment, develop an enterprise plan for rolling out the archiving capability.
- **Approach 2:** Start with a pilot effort to validate the cost savings that can be realized by application data archiving. Then conduct an enterprise-wide assessment and develop the roadmap for expanding data archiving.

Contractor recommends Approach 2 because this provides the opportunity for a quick win to both measure the impact of data archiving and to demonstrate its potential to support additional applications across the County. Also, it reduces the near-term investment in hardware and software. Finally, it helps to better define the County's true requirements, which reduces the potential risk of oversizing the enterprise archiving environment.

- Description of solution to meet the requirements

Contractor sees this initiative focusing primarily on applications that have structured, rather than unstructured, data sources. Recognizing that not all applications have the same potential for data archiving, Contractor would focus on database-to-database archiving as the primary archive model.

A component of the Contractor's Information Management/Information Governance (IM/IG) Portfolio is the Structured Data Manager (SDM) tool. SDM automates application lifecycle management and structured data optimization by relocating inactive data from expensive production systems and legacy databases, while preserving data integrity and access. SDM enables retiring outdated applications through an automated process of extracting, validating, and deleting data.

Rationale: This unique solution significantly reduces capital expenses and administrative costs, and helps the County to respond quickly to legal and compliance requests. This enables the County to obtain maximum value from the data.

Timing: This initiative can begin at any time after Contract Effective Date (CED); however, Contractor recommends beginning this initiative after completion of Transition. This would make sure that all changes to the data center architecture are complete and would reduce the complexity of implementation.

Risk Considerations: Each application would have to be assessed and evaluated independently to determine the value of archiving data. There is a risk of overestimating the impact of application data archiving, leading to over-solutioning the archiving platform. Contractor addresses this risk by starting with a pilot effort for a single application that meets a common profile for successful archiving. Contractor would also assist the County to assess other applications and prioritize them for archiving based on the potential for storage or other savings.

Key Dependencies: There are no real dependencies—in fact, the County considered a pilot effort in 2015. However, as stated above, Contractor would recommend delaying the start of this initiative until after completion of the Transition phase of the Agreement.

Milestones: Key milestones for this initiative include the following:

- Milestone 1 – SDM Requirements and Analysis
- Milestone 2 – Architecture and Solution Design
- Milestone 3 – Foundation Build in Development/Test Environment
- Milestone 4 – Onboarding and Archiving of the Central Reporting System (CRS) Tax Data
- Milestone 6 – Knowledge Transfer and Testing
- Milestone 7 – Foundation Build in Production Environment
- Milestone 8 – Post Production Support and Documentation

- Deployment plan for resources and use of facilities

Contractor would initially provide a team of SMEs to guide the planning and piloting efforts. This team would collaborative onsite with the County's staff and the local support to define requirements and to validate the results of the project. The team would also conduct knowledge transfer to facilitate extending the implementation and support County-wide. Contractor SMEs would remain available as required to provide reachback support.

- Key methodologies and processes in solution

The County has in excess of 400 applications. The potential value for archiving portfolio data varies significantly from one application to another. Contractor recommends conducting a pilot effort on one of the County's applications to validate the potential for reducing application data storage requirements rather than starting with a County-wide implementation of Portfolio Application Archiving.

Previously, the County, with the support of Contractor, identified Treasurer-Tax Collector (TTC) CRS as a candidate for the pilot effort. Following the pilot, Contractor would work with the County to develop a strategy and roadmap for extending application data archiving to other County applications.

- Automated systems and tools involved in solution

Contractor plans to use the SDM tool, described above, to reduce the data footprint of the County's structured data. SDM software comprises an integrated set of components that facilitate design, deployment, and ongoing management of archiving processes throughout the lifecycle of applications and data. In addition, they deliver capabilities that address different levels of application complexity, data volumes, and archive access requirements. The components include the following:

- Designer – Provides a visual interface to model data and create business-aligned data migration rules with ease
- Data movement – Makes sure data relocation is performed to meet volume requirements while retaining application integrity at all times
- Archive access – Provides a full range of access capabilities to meet requirements for business operations, regulatory compliance, and legal discovery
- Job engine – Automates all archiving tasks with built-in recovery and restart
- Management console – Provides system configuration, job monitoring, job launching, and complete audit trail capabilities

- Key Considerations and Potential Alternative Approaches

Hyperconverged Integrated Systems: Hyperconverged infrastructure is designed to simplify the design and management of the computing environment by merging and pre-packaging the server, network, and storage components of infrastructure into pre-sized building blocks. To deliver the most value, hyperconverged systems would have to comprise nearly all of the infrastructure deployed in the data center; otherwise, the hyperconverged solution becomes just another platform that has to be integrated and adapted to existing standards; this would increase rather than decrease overall complexity in the environment.

One possible application of hyperconvergence that the County could consider in the shorter term would be the implementation of hyperconverged infrastructure for servers deployed in County field sites. As systems come up for refresh, Contractor would compare available options in the marketplace for cost, compatibility with established management tools and fielded applications, and if a hyperconverged solution would yield benefits to the County, Contractor would recommend its implementation.

- Description of solution to meet the requirements

Contractor would implement Helion MPC and Helion Managed Cloud Broker (HMCB) during the Transition as Contractor builds the County's on-demand Dev/Test and Production environments as part of the data center consolidation. These platforms start the County on a path of greater standardization in the virtual/converged infrastructure environment. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, Contractor would be able to test and validate whether a hyperconverged infrastructure would ultimately yield benefits for the County.

When the County is ready for hyperconvergence, Contractor would provide the technology partnership to achieve this. If Contractor is able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step is to plan, design, and implement a hyperconverged infrastructure. During the planning phase Contractor would build the business case for hyperconvergence and would provide the County with alternative solution designs built on the most suitable and current technology and vendors available. HPE offers a wide range of hyperconverged systems that Contractor continues to advance and innovate with to suit various business cases and client needs.

To achieve the best possible outcomes from the County's investment in this technology and to meet its needs in a way that helps to better support County business, Contractor would consider and evaluate the following features to help the County select the optimal hyperconverged solution:

- **Integration for Seamless Coexistence**. Ability of the hyperconverged solution to integrate with the legacy environment. The hyperconverged solution must enable the County to fully integrate the new solution with the legacy environment. Existing server and storage assets must be able to coexist with the new environment until the eventual collapse of multiple administrative interfaces into fewer simpler tools.
- **Scalability**. Ability to grow the environment in a non-disruptive manner and the ability to scale up or scale out without replacing the initial equipment with new equipment. The solution must offer just-in-time growth capability to avoid the need to carry expensive inventory. Additionally, granularity in scalability is important to scale only the resources required in the increments that make sense for the County.
- **Data Mobility**. Ability to move data around to accommodate individual device outages—the ability to easily move data between the hyperconverged platform and other systems, without having to rely on consultants.
- **Data Protection**. Ability to protect data in the event of hardware failures, human error, or natural and manmade disasters while meeting desired SLAs, RPOs, and RTOs without the need for an additional software or hardware layer. Features Contractor would evaluate for the County include RAID or mirroring, fault tolerance, replication (synchronous and asynchronous) within the site and between sites as well as full disaster recovery capabilities.
- **Performance**. Ability to provide performance opportunities that are considered enterprise-class. This means that the solution is to support flash and, optionally, spinning disk. Ideally, both would be supported because they have different strengths and weaknesses. When it makes sense, the solution should be able to automatically tier storage systems to enable faster data access or, at the very least, have an accelerated method for handling data retrieval.

- **Availability**. Ability to provide availability at SLA levels that meet County requirements for all systems. To determine this, Contractor would evaluate ease of scalability, ease of management, ability to scale out storage, tolerance for node loss, cluster resiliency, and capabilities of automated failover.

Once Contractor has identified and received County approval of the plan, in a parallel but fully integrated mode of operation Contractor would execute a phased migration of the County's systems to the new hyperconverged infrastructure. Contractor's plan would also consider data center component refresh dates to maximize investments in the legacy environment prior to the migration.

Timing: Preparation for implementation of a hyperconverged infrastructure would occur during transition. Contractor recommends the actual implementation to occur as data center components come up for refresh.

Risk: None at this time.

Dependencies and Milestones:

- Prior to the County investing in a hyperconverged integrated solution, standardization on the Managed Private Cloud platform must be established
- To migrate to a hyperconverged infrastructure, existing legacy equipment would need to be refreshed onto the hyperconverged platform.
- Development of implementation strategy and plan.

- Key methodologies and processes in solution

With the implementation of hyperconverged systems, methodologies and process for deployment become easier as a result of the pre-configuration of server, network, and storage components of infrastructure into pre-sized building blocks. These systems include easy-to-use management tools designed to streamline implementation and management and help shield the administrator from much of the underlying architectural complexity.

Contractor's new hyperconverged systems deploy VMs in just five clicks, update hardware and firmware in just three clicks, and provide instant diagnostics and analytics to enable faster response to business needs.

- Deployment plan for resources and use of facilities

Contractor's facility approach is to deploy the new hyperconverged infrastructure at Contractor's primary data center in Tulsa, Oklahoma and/or in field sites as deemed appropriate.

- Automated systems and tools involved in solution

Contractor's vision is to dramatically simplify and streamline IT administration and operations management. While many hyperconverged integrated system solutions are available on the market today, Contractor is a market leader in hyperconverged systems. Contractor's hyperconverged systems offer an infrastructure that provides the following features/benefits:

- Rapid provisioning of VMs
- Flexibility and speed to add capacity in as little as 15 minutes
- Simple IT operations with firmware and driver updates in just three clicks
- 99.999% continuous data availability
- Federated lifecycle management
- Data fabric with data mobility across systems, sites, and cloud
- Lower startup cost with two-node entry and linear scaling
- 62% lower cost for disaster recovery
- Pay-as-you-grow flexible capacity model

Using HPE OneView as the common software-defined convergence platform, Contractor provides software-defined management for both Contractor's larger ConvergedSystem 700 powered by Intel models as well as the smaller CS200-HC models. The HPE OneView End-User experience (UX) makes managing and monitoring systems so easy, no manual is required. HPE OneView integrates with HPE Helion OpenStack and CloudSystem and has extensions to a variety of management software. With a commitment to provide clients with the most flexibility, Contractor has been continually and significantly expanding this ecosystem since 2015.

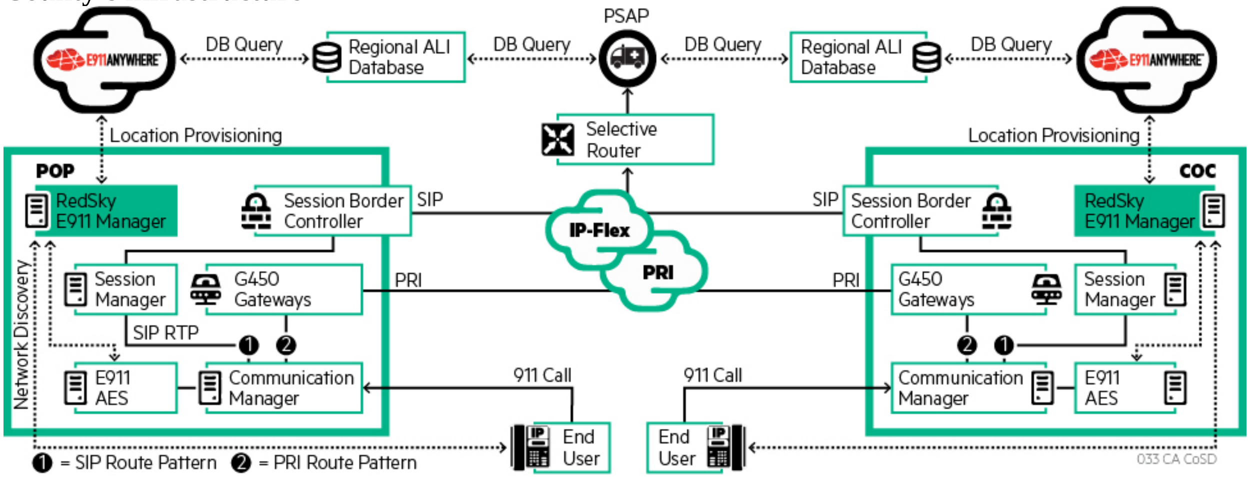
E911 Transformation Project

- Description of solution to meet the requirements

The solution highlighted in this section specifies the E-911 migration planned for implementation early in the Agreement at existing VoIP sites and ongoing in parallel with VoIP site upgrades.

Contractor recommends the adoption of the industry leading E911 Manager and E911 Anywhere by RedSky technologies. RedSky's E911 Manager® solution would be implemented in line with the County's geo-redundant network core, with infrastructure at the AT&T Point of Presence (POP) and the County Operations Center (COC). The primary application would run on an active host with a standby host that would take over in the event of failure of the primary server, enabling full redundancy.

Fully-integrated E911 solution would automate the E911 process by recognizing route patterns within the County's infrastructure



The E911 Manager would *automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager via the AT&T MPLS network to track and update phone moves, adds and changes.*

To handle the growing deployment of VoIP services throughout the County, RedSky's E911 Manager would communicate with the Avaya Enterprise voice network to monitor registration events of VoIP endpoints. E911 Manager would use Layer 2 Network Discovery or Layer 3 Network Regions to determine the location of the End-User based on port, network device, or IP address and would update the Avaya Communication Managers with the proper Emergency Line Identification Number (ELIN) for 9-1-1 off-net calling. The E911 Manager server would create and store Automatic Location Identification (ALI) records as necessary and submit to RedSky's E911 Anywhere® cloud service in the required format for the local Public Safety Answering Point (PSAP).

To manage ALI information centrally—for County locations or to support mobile softphone users—the RedSky solution includes RedSky E911 Anywhere cloud service. E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 PSAPs in the USA and Canada. E911 Anywhere is an effective choice for the County based on its distributed locations as well as the increase in mobile and desktop IP softphone users. The recommended solution by AT&T would feature the following:

- A fully automated E911 solution that would track the location of phones as phones move within the County's enterprise voice network
- An E911 software application located at the AT&T IDC and COC that would interface with the Geo-Redundant Avaya Communication Manager voice network
- A solution that connects with all Private Switch-Automatic Location (PS-ALI) Identification databases throughout the cities within the County
- A solution that provides Emergency On-Site notification to anyone working at the County of the location of a call placed to 9-1-1
- Geo-Redundant Active / Active Server construct located at the AT&T Internet Data Center (IDC) and COC for high availability and redundancy
- Reporting and metrics for auditing of all E911 activity
- As a "cloud-based" 9-1-1 call routing service, E911 Anywhere can send a 9-1-1 call to any PSAP in the U.S. or Canada (with County approval)

E911 is a necessity for the County enterprise VoIP deployment. As stated in the introduction, this solution would be integrated into the County's enterprise-wide VoIP migration, enabling functionality on a site-by-site basis over the length of the transformation initiative.

- Deployment plan for resources and use of facilities

For the e911 solution, Contractor shall ensure that AT&T leverages the local LCM (Life Cycle Management) team, in-house vendors, direct manufacturers, and carriers. Contractor shall ensure that AT&T personnel provides this support from its location on Trade Street in San Diego.

- Key methodologies and processes in solution

All support services—whether triage, new requests, change requests, or removals—are initiated by the County End-User to the Contractor Service Desk. All requests within the network framework for E911services would be directed to the AT&T LCM team for assessment and completion.

AT&T would leverage the RedSky's solution for updates to the PSAP routing and PS-ALI databases as County staff request Adds, Moves or Changes to their VoIP telephone stations. The tracking of VoIP phones is made possible by enabling Layer 3 Network Regions on the County's LAN. This is the most common method of tracking IP, SIP, and IP soft phones inside an enterprise. This method, which is specific to Network Regions or subnets, establishes a dedicated block of IP addresses associated to the region at the DHCP server. Each Network Region would then have assigned to it a physical address and an ELIN. Every time a VoIP phone registers to the Avaya Call Manager at the AT&T POP or County Operations Center, E911 Manager reviews the IP address of the VoIP phone to determine if the IP address falls into one of the IP address ranges set aside for the regions. If E911 Manager determines that a VoIP phone is in a Network Region, E911 Manager would provide the ELIN to the respective Avaya Communication Manager server at the AT&T POP or County Operations Center.

- Automated systems and tools involved in solution

E911 Manager solution would automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T Multiprotocol Label Switching (MPLS) network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

Identity Federated Services Transformation Project

- Description of solution to meet the requirements

Contractor analyzed Okta, Oracle, and IAMaaS during the technology selection stage and recommended HPE's IAMaaS due to the maturity of the product and services, purchase and maintenance cost, and lower risk during implementation. However, if the County opts for another solution such as Okta or Oracle, Contractor would work with the County to plan and execute a successful implementation of either vendor's solution.

The recommended Identity Federated Services solution includes the following components:

- The existing Oracle IDAM technology platform as its core
- Microsoft Active Directory Federation Services (ADFS)
- HPE's IAMaaS to enable the federation services where the County is acting as service provider and identity provider.

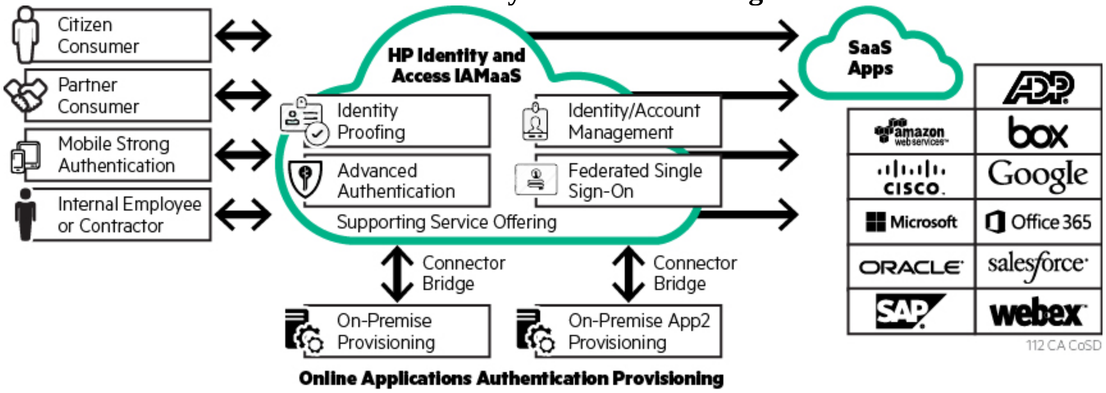
Contractor would use IAMaaS to integrate external constituents within the County's Identity Management Service. IAMaaS is a cloud-based IDAM) solution built using the Computer Associates (CA) secure cloud product for multi-tenancy. IAMaaS is hosted on the HPE Helion Managed Virtual Private Cloud for U.S. Public Sector. The following elements describe the main features of the IAMaaS solution and how they relate to the County:

- User life cycle management such as self-registration, password resets, and profile updates.
- Application access management to request access to applications.
- Hybrid provisioning cloud and on premise to create/update on-premise identity requirements.
- Identity synchronization on premise to make certain that relevant data is updated one way or bi-directionally.
- Reporting for compliance and audit.
- Identity proofing from the solution to County data stores.
- The single sign-on (SSO) Federation Hub can act as identity provider (IDP) and service provider (SP) to County software as a service (SaaS) applications.
- IAMaaS can act as a Federation Hub. External users can be authenticated to SaaS apps using their County/IAMaaS credentials, County credentials, or social login credentials like Facebook.
- The CA Security SaaS Validation Program helps SaaS vendors increase sales and adoption by simplifying and validating their SSO interoperability. It enables smooth integration of SaaS solutions into CA SSO environments in an End-User-friendly and cost-effective way.
- Credentials may include Forms, Integrated Windows Authentication (IWA), multi-factor authentication (MFA), public key infrastructure (PKI), Radius, OAuth, one-time password (OTP), and Risk.

The figure below illustrates the main elements of the IAMaaS solution and its relationship with the County, its citizens, employees, and partners. On the left side is each type of End-User who would interact with the service. Within the core or "cloud" of IAMaaS are the key services provided such as identity proofing, identity and account management, federated SSO, and advanced authentication. The resources and services to access are on the right; those services are both internal and external to the County IT environment, including third-party providers. Connectivity to the resources via the IAMaaS are enabled via industry-standard IDAM protocols.

IAMaaS solution

Contractor Identity and Access Management



Providing secure IT services operations through robust End-User identity authentication.

Rationale: Contractor believes that expanding the current IDAM capability along with implementation of HPE's IAMaaS for identity management of external users provides the most cost-effective solution. This approach *provides a low risk, non-disruptive method* to expand on existing County investments and meets the County's architecture vision for identity management.

Timing: The timing for expansion of the existing County IDAM solution to include federation would coincide with the ConnectWellSD project or other timing as required by the County. Other elements of the solution such as federation requests to business partners would occur as the solution is deployed.

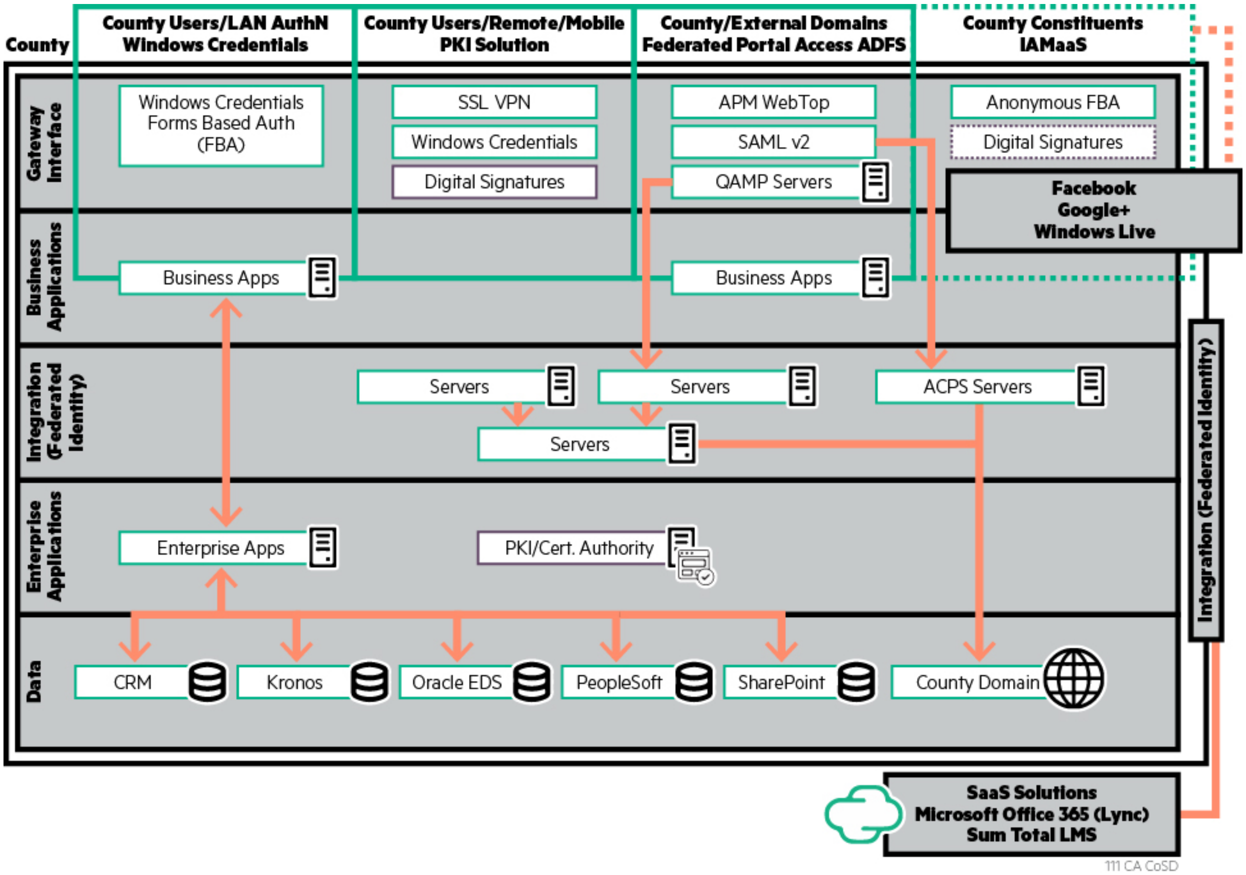
The figure below depicts the overall view of the IDAM solution and how Oracle, ADFS, and the HPE's IAMaaS would work together to provide identity federation. As seen in the figure, the core elements of the IDAM solution would work together to enable seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

The County ADFS 2.0 environment—a key component of the Identity Federated Services—has been operational since 2011, providing secured identity federation and web SSO capabilities for County and external business unit End-Users who require access ADFS-secured applications within the County network and in the cloud.

Earlier in 2016, the ADFS environment was upgraded to v3.0 with redundancy, and included a new test environment. By adding external access to the test ADFS server, this upgrade provides expanded use of the ADFS test environment for development and testing of new ADFS-secured applications.

Upgrading the ADFS environment was part of the County's overall IT roadmap to refresh and improve key infrastructure components and expand the County's IDAM solution. The key point is that this solution is strongly tied to the Identity and Access Management Services solution; it is a continuation of that capability but expanded to enable federation—much of the approach is duplicative.

The IDAM solution integrates Oracle, ADFS, and the HPE's IAMaaS



This solution offers minimal risk to the County and enables seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

Key Dependencies and Milestones: As a part of the overall IDAM effort, Identity Federated Services is encapsulated in the following list, which details the progressive steps of the IDAM solution and details what is being done today and what Contractor would perform in the future:

- Current/on-going effort – Oracle Federation Manager is currently deployed with Service Provider active and Identity Provider not active. Based on an existing request from the Department of Child Support Services (DCSS), Contractor plans to implement the Federation Acting as Identity Provider upon approval. To deliver the federation capability for DCSS, IAMaaS needs to be implemented simultaneously with Federation Acting as Identity Provider.
- Future – Develop a process for auto-onboarding new employees based on the information in PeopleSoft to create the Active Directory (AD) identities
- Future – Expand use of the existing platforms into all County business units and partners as well as work with the current Knowledge Integration Project (KIP) team (IBM) to expand to partners
- Future – Use Contractor's IAMaaS solution to expand to County residents and to act as the identity manager for County residents
- Future – Re-architect the solution to become a zero downtime solution
- Future – Federate with County third-party vendor applications

- Deployment plan for resources and use of facilities

Ongoing support for the IDAM service would be delivered by continental U.S.-based delivery resources in line with the County's requirements. With more than 5,000 security professionals who have IDAM expertise, Contractor has the experience to deliver even the most complex solutions.

The Contractor Tulsa Data Center would be the production data center, with the IDAM solution delivered from this location. This includes almost all web, application, and database servers, data storage, and data management. The Contractor disaster recovery (DR) site in Colorado Springs would provide the recovery site for the IDAM solution.

- Key methodologies and processes in solution

Contractor would adhere to the following key processes to deliver Identity Federated Services:

Solution Methodology: By incorporating the Contractor's IT Strategy & Architecture (ITSA) for Identity Federated Services, Contractor would take the same iterative approach, addressing issues and improvements in data quality and data management—in both practice and implementation. Through this process, Contractor would work closely with County data teams and other Contractor Transformation, Integration, and Architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. ITSA for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology.

In addition to the ITSA, Contractor would use standard TOGAF (The Open Group Architecture Framework)-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is documented correctly and that it also would lower the overall implementation risk to County. Contractor would integrate these key methodologies with the County's current Architecture and Solution reviews in conjunction with the County Technology Office (CTO) and relevant County groups.

For the Oracle IDAM Suite, Contractor would work with Contractor's IDAM architect to make certain that the design, development, and deployment of the Oracle suite follow standard Oracle design and deployment methods. This would facilitate operation of the Oracle platform within the design parameters. Any significant design changes to the platform or changes to the Oracle databases would follow Oracle mandated practices.

- Automated systems and tools involved in solution

Contractor would use the Oracle and Microsoft tools identified in the table below in support of Identity Federated Services.

Automated Tools for Support of Identity Federated Services

TOOL	PURPOSE
Identity Manager	• Oracle Identity Manager is designed to manage End-User access privileges across all of the County's resources, throughout the entire identity management lifecycle—from initial creation of access privileges to dynamically adapting to changes in business requirements. Identity Manager enables the incorporation of necessary business changes at minimal cost, while avoiding enforced customization.
Access Manager	• Oracle Access Manager provides adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization extended to mobile clients and mobile applications. Services can be licensed and enabled as required to meet the specific needs of the County.

TOOL	PURPOSE
Federation Manager	• Oracle Identity Federation (OIF) provides secure identity information exchange between external/internal partners. OIF provides account management for partner identities and integrations through support of industry federation standards. OIF protects existing IT investments by integrating with a wide variety of data stores, End-User directories, authentication providers, and applications.
Virtual Directory, Unified Directory	• Oracle Virtual Directory provides Internet and industry-standard Lightweight Directory Access Protocol (LDAP) and eXtensible Markup Language (XML) views of existing enterprise identity information without synchronizing or moving data from its native locations.
Microsoft tools and services also be used: • Microsoft Active Directory 2012 • Microsoft ADFS	• Microsoft Active Directory (2012) Domain Services (AD DS) provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network—such as users, computers, and other devices—into a hierarchical containment structure. The hierarchical containment structure includes the AD forest, domains in the forest, and organizational units (OUs) in each domain. • ADFS (Active Directory Federated Services) provide County users with SSO access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and to implement federated identity. (Claims-based authentication involves authenticating an End-User based on a set of claims about that End-User's identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the End-User by other means, and that is trusted by the entity doing the claims-based authentication.) It is part of the AD DS.

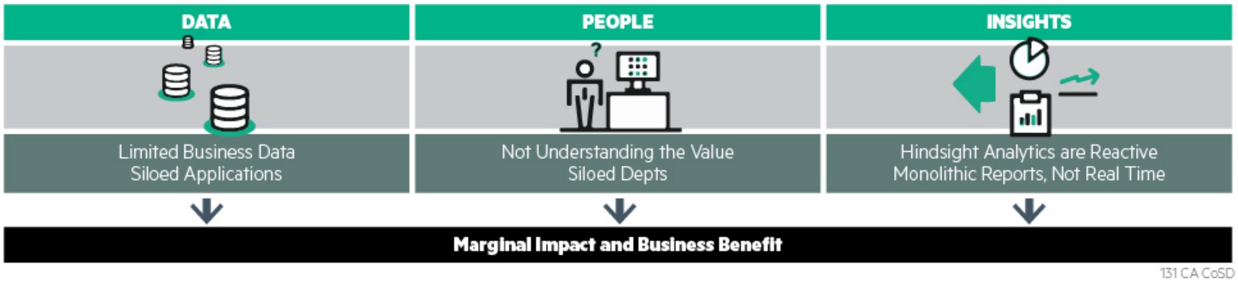
Enterprise Information Management Transformation Project

- Key Considerations and Potential Alternative Approaches

Contractor recommends implementation of an Enterprise Information Management (EIM) program to capitalize on the valuable data that is available but currently not harnessed. This shall provide the County with information it needs to make more informed decisions and present an enterprise view of the data that could be used to make richer programs available to the public.

The County has begun the journey to modernize the Information Architecture and Governance model a critical step as modernization and transformation of the IT infrastructure begins. The information architecture must address traditional "feeds and speeds," and include business definitions of information and the information processes to incorporate all data (structured, semi-structured, and unstructured (xml, flat files, scanner files).

Siloed business data, as shown in the figure below makes it difficult to take full advantage of the information available across the enterprise. To the County, this could mean employees are limited in their ability to perform certain job functions or provide the services citizens need. This can result in added frustration for both employees and citzens.


DATA
PEOPLE
INSIGHTS
Limited Business Data
Siloed Applications
Not Understanding the Value
Siloed Depts
Hindsight Analytics are Reactive
Monolithic Reports, Not Real Time
Marginal Impact and Business Benefit
131 CA CoSD

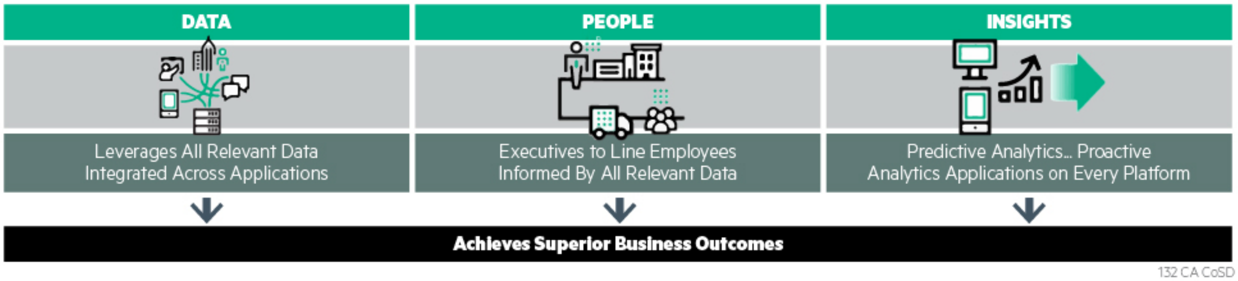
When data is siloed, it is more difficult and time consuming for County employees to find the information needed to support citizens.

EIM provides an essential framework for managing and governing information (data) across the enterprise and requires:

- Governance and stewardship
- Integration
- Methodologies and standards
- Architecture and technologies
- Enterprise data models

The payoff for an EIM solution is clear—the County would be better prepared to more rapidly meet the needs of employees and citizens by gaining greater insight from the data it collects, as shown in the figure below.

Integrated Data Across the Enterprise.


DATA
PEOPLE
INSIGHTS
Leverages All Relevant Data
Integrated Across Applications
Executives to Line Employees
Informed By All Relevant Data
Predictive Analytics... Proactive
Analytics Applications on Every Platform
Achieves Superior Business Outcomes
132 CA CoSD

Easy access to all available data facilitates decision making and helps to achieve superior business outcomes.

As Contractor and the County develop a modernized Information Architecture and Governance model, Contractor would consider a wide-range of common challenges that include:

- Inconsistent definitions of key business data, leading to incomplete, incorrect business metrics
- Information that is not available, incomplete, inaccurate, and untimely to enable informed business decision
- Time-consuming, manual processes, adding to employee workload and citizen frustration
- Fragmented data, preventing or delaying comprehensive situational analysis and appropriate actions
- Siloed project work, preventing integration or extension across enterprise
- Inconsistent data, preventing standardization and reuse of processes, methods, among others
- Siloed decision making, which may be counterproductive to the enterprise
- Poor data quality and fragmented data security/auditability, exposing compliance risks (SOXA, HIPAA, ISSA, CCA, FRCP, Basel II Accord, PCI, EU Privacy Directive, etc.)
- Unknown data retention needs/requirements, transforming data assets into data liabilities (storage costs & exposure risks).

Contractor recommends EIM for developing a coherent and supportable Information Architecture and Governance model. This approach would focus on developing an information strategy and a roadmap for implementing the strategy, and then to invest in delivering the supporting initiatives.

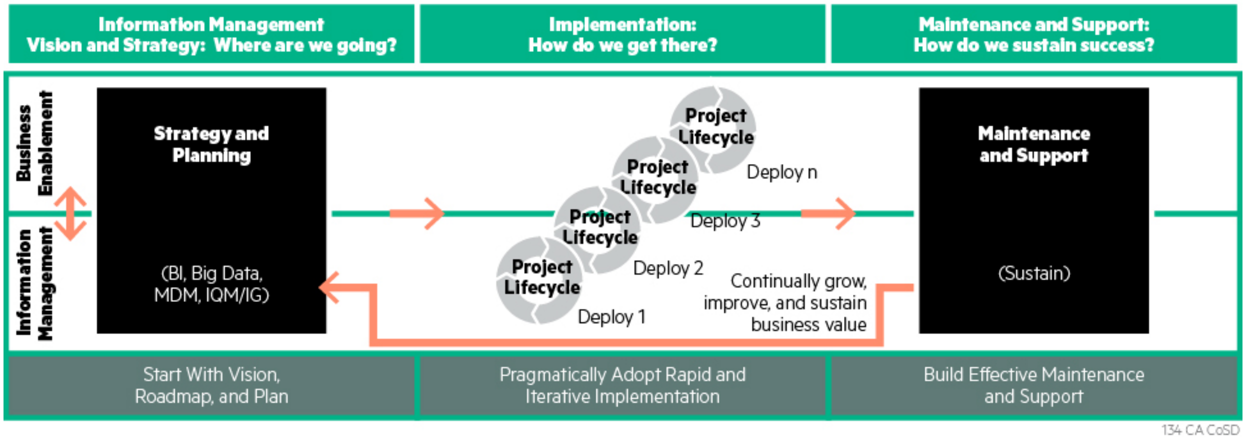
- Description of solution to meet the requirements

Contractor proposes a two-phased approach to establish a coherent EIM program. The first phase is a stand alone project. This project focuses on the objective defining the County's EIM program. Key deliverables from this project include: Vision and Strategy Document and EIM Roadmap.

The second phase is would consist of a number of separate projects detailed in the Roadmap from Phase 1. Each project would have well defined objectives and deliverables defined throughout the implementation process. Specific intitiatives/projects identified in the roadmap are executed in a rapid and iterative approach. Contractor scopes the implementation projects upon completion of the vision and strategy. Projects associated with the second phase would be completed via work request.

The figure below illustrates the Contractor approach to EIM. Of particular note, Contractor's approach is to address and align business enablement with information management.

Contractor Approach to EIM



Contractor's approach aligns business enablement and information management that address true business needs.

Rationale: EIM provides the framework for managing and governing information across the enterprise. An EIM program enables data sharing for better decision making and provides County leaders with insight into to the quality of services that they deliver to their citizens.

Timing: Contractor estimates the time required to develop the information management vision and strategy and roadmap to be a 3- to 4- month period that would occur after transition. Contractor would work with the County to determine the business needs and to document the supporting technical requirements. To minimize the County's time investment, while maximizing impact, Contractor would conduct information gathering through a series of focused discussions with stakeholders. This helps Contractor to have an accurate understanding of the current environment as well as the desired future state. At the end of this effort, Contractor would deliver a strategy and roadmap for review and approval by the County.

Risks: None identified.

Dependencies: Developing an effective EIM program is dependent on the active involvement of the business groups as well as the CTO.

Milestones: Key milestones in the planning and implementation of EIM include the following:

- **Milestone 1 – Business Needs Assessment.** A core component of the information gathering phase of the strategy and vision project that focuses on the needs of the business in terms of EIM.
- **Milestone 2 – Current State Assessment.** The second core component of the information gathering phase focuses on documenting the existing technical environment to support EIM
- **Milestone 3 – Desired State Gap Analysis.** The transition step into analysis and planning phase where Contractor documents the gaps between what the County's business needs are and the current technical environment.
- **Milestone 4 – Strawman Vision and Roadmap**. This milestone reflects Contractor draft strategy and roadmap for the County.
- **Milestone 5 – Final Vision and Roadmap.** Once the County reviews and approves, Contractor provides the final strategy and roadmap to guide implementation the of EIM program.

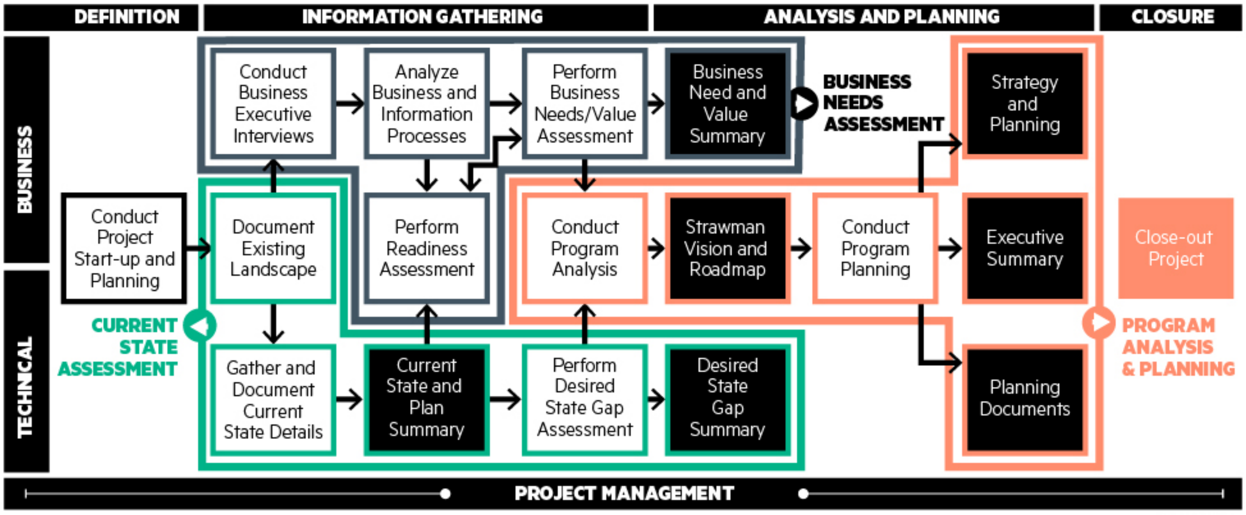
- Deployment plan for resources and use of facilities

For the development of the County's Information Management Strategy, Vision, and the supporting Roadmap, Contractor provides a small team of experienced consultants to work on-site in San Diego with the local support team and key County stakeholders.

- Key methodologies and processes in solution

During the past 40 years, Contractor has developed and documented its IT Solution Architecture (ITSA). This methodology. This methodology would provide the foundation for Contractor's EIM solution. The figure below identifies the detailed steps for both the development of strategy and vision and implementation.

Contractor Global Methods for Information Strategy Master Plan


DEFINITION
INFORMATION GATHERING
ANALYSIS AND PLANNING
CLOSURE
BUSINESS
TECHNICAL
Conduct Business Executive Interviews
Analyze Business and Information Processes
Perform Business Needs/Value Assessment
Business Need and Value Summary
BUSINESS NEEDS ASSESSMENT
Strategy and Planning
Conduct Project Start-up and Planning
Document Existing Landscape
Perform Readiness Assessment
Conduct Program Analysis
Strawman Vision and Roadmap
Conduct Program Planning
Executive Summary
Close-out Project
CURRENT STATE ASSESSMENT
PROGRAM ANALYSIS & PLANNING
Gather and Document Current State Details
Current State and Plan Summary
Perform Desired State Gap Assessment
Desired State Gap Summary
Planning Documents
PROJECT MANAGEMENT
133 CA CoSD

Contractor uses a collaborative approach to identify and document requirements and gain concurrence for the way forward.

The methodology uses a collaborative approach to align business needs with technology by documenting the current state of technology, process and strategy. Through structured information gathering Contractor documents the desired state and analyze of this information to identify gaps between the current state and the desired state. Contractor uses this information to develop the roadmap to address the gaps. Each step in the framework results in detailed artifacts tailored to the County. Contractor's consultants are trained on the methodology and are experienced in guiding the process, making sure that the County's experience is positive and the results meet their information management needs.

While not included in the proposed initiative, Contractor anticipates that after the County develops its EIM strategy and roadmap, there would be a need to support implementation of EIM. Contractor has a mature methodology for implementation and is prepared to support the County in this phase. This methodology applies proven templates and suggests industry best practices to gather the correct information needed for successful implementation. Contractor would work with Contractor's account team and provide Contractor's expertise to help guide project implementation as identified in the County roadmap. Common implementation projects address information management/quality, master data management, information governance, enterprise data modeling, and development of enterprise standards.

- Automated systems and tools involved in solution

The process for planning and implementing EIM projects relies on standardized templates to gather and document requirements. These result in well-defined deliverables that are guided by an extensive set of artifacts and knowledge libraries. Contractor would use its existing methodologies and associated processes to develop the strategy and plan. As Contractor assesses the current environment and conduct a gap analysis, Contractor documents technology requirements for subsequent implementation projects.

Comprehensive Applications Threat Analysis (CATA) Service Transformation Project

- Description of solution to meet the requirements

Contractor's Comprehensive Applications Threat Analysis (CATA) service uses well-established return on investment (ROI) practices for quality improvement. These practices demonstrate that fixing defects after code implementation can be 30 to 100 times costlier than discovering, avoiding, or reducing the severity of defects early, during requirements analysis, architecture, and design. Conventional software development practices discover and fix only a small fraction of security vulnerabilities later in the application development life cycle; CATA enables achievement of a much higher level of assurance with security and lower rework costs. CATA minimizes security-related rework by helping get it right the first time by identifying security issues in higher layers of abstraction of the application (requirements, architecture, design). This can pervasively improve applications security to complement other efforts to address security issues in source code (static) and run-time behavior (dynamic).

Projects: CATA reviews would be conducted on a subset of the County's applications, selected and prioritized according to factors such as County-provided priority, sensitivity/criticality of data managed by application, impact if the application is compromised (confidentiality, integrity, or availability), significance/scope of application updates (especially new requirements, updated architecture, design, transformation/modernization), any available risk characterizations, and other factors agreed to by Contractor and the County. Likewise, prioritization criteria and decisions would be made for static security code reviews and applications vulnerability assessment and penetration testing. In cases where a CATA review is conducted, and it is deemed appropriate to conduct a follow-on CATA review on the same application (for instance, above the risk prioritization threshold for CATA reviews, and having another major release since prior review), a CATA delta review would be conducted, starting with the CATA baseline analysis initially performed or a prior CATA delta review.

Objectives: the identification of security requirements/controls gaps and vulnerability risks, and recommendations to address (close gaps, lower risks) for each security assessment (CATA, static security code review, vulnerability assessment / penetration test) to improve the security of these applications by a prioritized incorporation of the review recommendations.

Deliverables: A prioritized and vetted list of security findings from each of two CATA phases (Security Requirements Gap Analysis; and Architectural Threat Analysis) with project team commitments to address factored into before and after severities. These can be in the form of summary slides (most common form of deliverable), samples of which are shown below in the Key Methodologies section, or longer written reports at the County's option, which include additional explanatory narrative and background on the specific analysis results that contributed to the findings. Findings from code review and vulnerability assessment and penetration testing are in the form of written reports describing findings, along with severities and remediation recommendations.

- Key methodologies and processes in solution

CATA is a two-phase activity—Security Requirements Gap Analysis and Architectural Threat Analysis—that includes interviews with Contractor development staff, analysis by Contractor staff and tools, and reporting.

The **Security Requirements Gap Analysis** determines security requirements and control gap for deployment of the application in compliance with applicable regulatory frameworks and industry best practices. The gap analysis would establish security control objectives and lay the groundwork for the threat analysis.

During the Security Requirements Gap Analysis phase, Contractor would identify relevant sources for security requirements derived from applicable regulatory requirements. Contractor then would establish traceability from the County’s regulatory or business environment to a prioritized set of security requirements. From the information Contractor gathers through Contractor’s proprietary templates and stakeholder interviews, Contractor would determine the plans and commitments for addressing these requirements, with special focus on already-designated technical solutions and already-documented security expectations, and the remaining gaps.

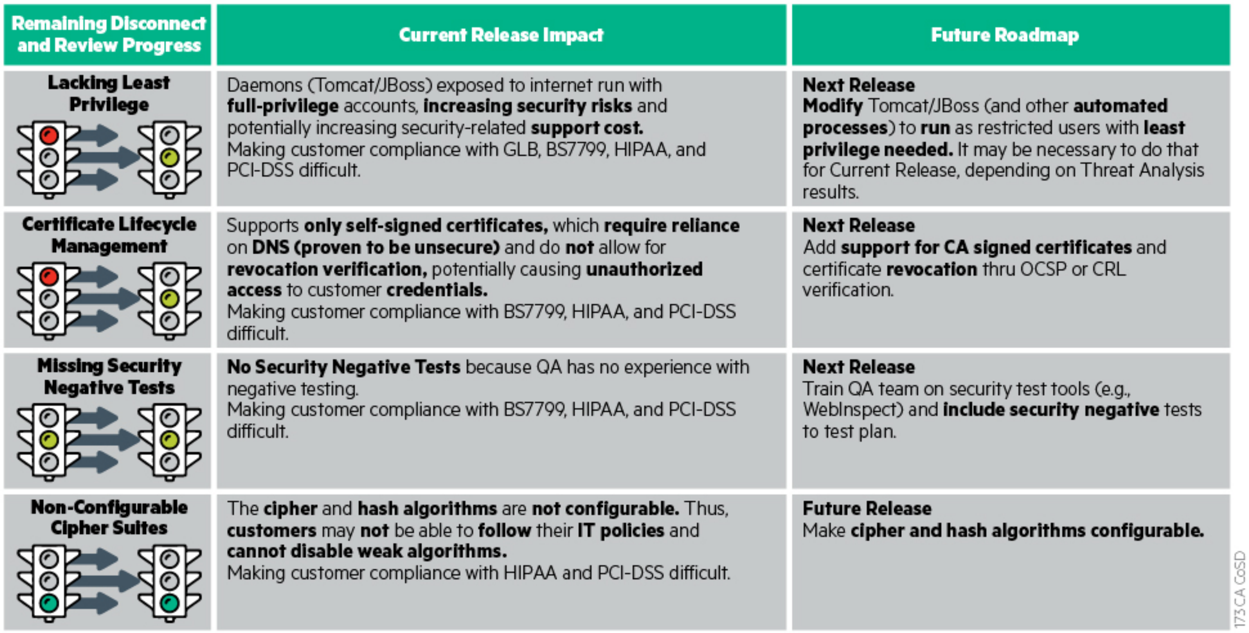
The Security Requirements Gap Analysis is based on:

- Expert system-like templates, with partially encoded expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers
- Efficient, repeatable results
- Requirements traceability from a robust collection of governance sources, including regulations, laws, and best practices.

The end result is a Security Requirements Gap Analysis that would identify important security requirements that may not be met through current plans. It places these at-risk requirements in priority or severity order.

The figure below is a sample of summary level Security Requirements Gap Analysis findings, which would be part of a larger findings slide deck.

Security Requirements Gap Analysis Sample Summary of Findings



Remaining Disconnect and Review Progress	Current Release Impact	Future Roadmap
Lacking Least Privilege	Daemons (Tomcat/JBoss) exposed to internet run with **full-privilege** accounts, **increasing security risks** and potentially increasing security-related **support cost.** Making customer compliance with GLB, BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** **Modify** Tomcat/JBoss (and other **automated processes**) to **run** as restricted users with **least privilege needed.** It may be necessary to do that for Current Release, depending on Threat Analysis results.
Certificate Lifecycle Management	Supports **only self-signed certificates,** which **require reliance** on **DNS (proven to be unsecure)** and do **not** allow for **revocation verification,** potentially causing **unauthorized access** to customer **credentials.** Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Add **support for CA signed certificates** and certificate **revocation** thru OCSP or CRL verification.
Missing Security Negative Tests	**No Security Negative Tests** because QA has no experience with negative testing. Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Train QA team on security test tools (e.g., WebInspect) and **include security negative** tests to test plan.
Non-Configurable Cipher Suites	The **cipher** and **hash algorithms** are **not configurable.** Thus, **customers** may **not** be able to **follow** their **IT policies** and **cannot disable weak algorithms.** Making customer compliance with HIPAA and PCI-DSS difficult.	**Future Release** Make **cipher and hash algorithms configurable.**

173 CA CoSD

This sample report shows an overall security assessment of Medium Risk from non-supported security requirements.

The **Architectural Threat Analysis** is an architecture-level review of the security properties of the underlying components and interfaces and provides recommendations for mitigating all identified moderate- and high-risk areas.

CATA combines information about the target application and deployment environment with target application security plans. A Contractor security consultant, uses CATA tools and templates that include a requirements traceability questionnaire and database, and an architectural threat analysis heuristic template. These tools add repeatability, semi-automated risk calculations, and serve as an "additional reviewer in the room." Contractor's security consultant then analyzes the resultant data.

In the Architectural Threat Analysis phase, the CATA team acts as an independent party, and would interview the designated Project Security Architect for the specified application or system. Contractor would then review architecture-level documents to gather information regarding architectural interfaces, components, data, and security characteristics, in addition to security mitigations already planned. Contractor has developed a repeatable process that uses a variety of well-established heuristics to identify interfaces and security properties that have the greatest risk of security defects. The Contractor analyst would factor in the risk reduction resulting from the mitigations and controls reportedly applied, and identify areas of residual elevated risk as well as technical control opportunities.

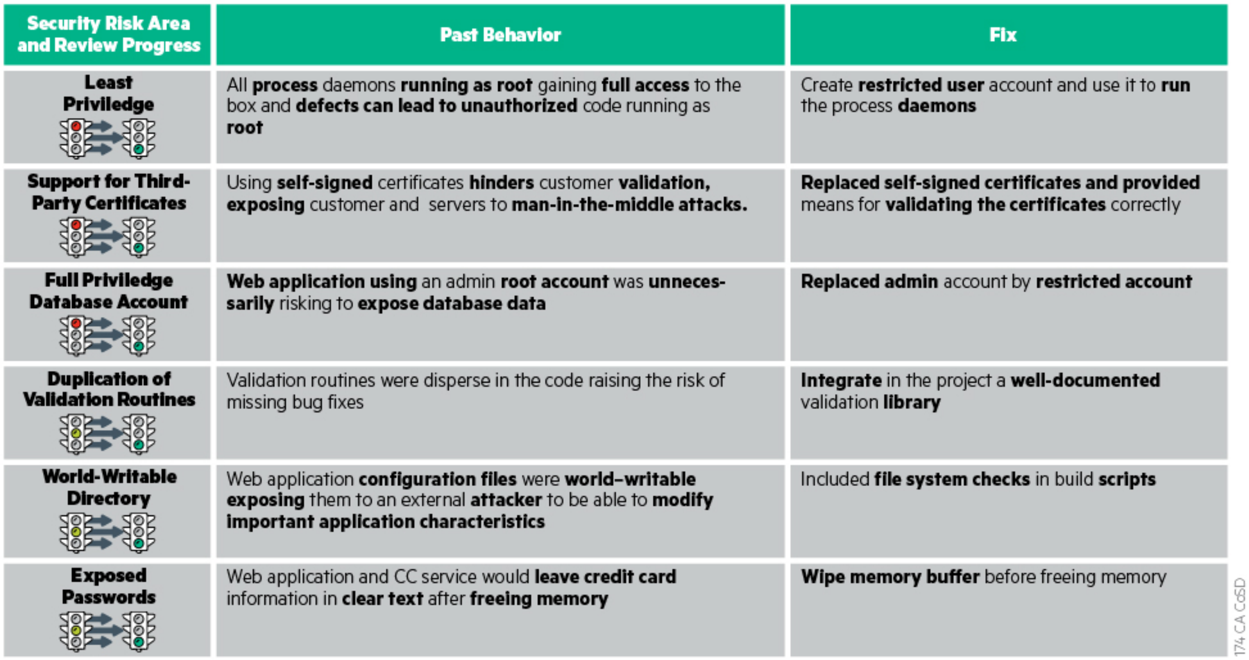
The Architectural Threat Analysis invariably finds unnecessarily elevated security risks that would benefit from additional technical controls. Contractor investigates specific solutions to address the security risks and provides recommendations based on best fit for the County's organization and mission. This task does not include implementation of the solutions. Architectural Threat Analysis can preempt building security flaws into applications based on the following elements:

- Expert system-like artifacts, encoded with first-order expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers

- Efficient, repeatable results.

The figure below is a sample of summary level Architectural Threat Analysis findings (part of a larger findings slide deck).

Sample Architectural Threat Analysis Report



Security Risk Area and Review Progress	Past Behavior	Fix
Least Priviledge 🟥 → 🟩	All **process** daemons **running as root** gaining **full access** to the box and **defects can lead to unauthorized** code running as **root**	Create **restricted user** account and use it to **run** the process **daemons**
Support for Third-Party Certificates 🟥 → 🟩	Using **self-signed** certificates **hinders** customer **validation, exposing** customer and servers to **man-in-the-middle attacks.**	**Replaced self-signed certificates and provided** means for **validating the certificates** correctly
Full Priviledge Database Account 🟥 → 🟩	**Web application using** an admin **root account** was **unnecessarily** risking to **expose database data**	**Replaced admin** account by **restricted account**
Duplication of Validation Routines 🟨 → 🟩	Validation routines were disperse in the code raising the risk of missing bug fixes	**Integrate** in the project a **well-documented** validation **library**
World-Writable Directory 🟨 → 🟩	Web application **configuration files** were **world-writable exposing** them to an external **attacker** to be able to **modify important application characteristics**	Included **file system checks** in build **scripts**
Exposed Passwords 🟨 → 🟩	Web application and CC service would **leave credit card** information in **clear text** after **freeing memory**	**Wipe memory buffer** before freeing memory

174 CA CdSD

The Architectural Threat Analysis prevents security risks from being introduced into application code.

Missing or incomplete security requirements, architectural threats, and/or previously investigated remediation may be identified during the analysis. Contractor would report these findings based on their severity: High (Red), Moderate (Yellow), and Low (Green). Severities can be modified if required to match specific regulatory frameworks.

Findings would include a high-level executive summary, slide tables of individual prioritized findings with remediation recommendations, and if a written report is required, a technical discussion section.

While CATA is highly effective for proactively identifying and mitigating potential security risks in the targeted applications, Contractor recommends combining CATA with secure code analysis by a security expert using the Fortify tool or with hybrid combinations such as Contractor's human expert security code reviews, in addition to Contractor's applications vulnerability assessment and penetration testing. This would result in identifying vulnerabilities through both static and dynamic security analysis, as these highly complement CATA. Static security analysis identifies issues in source code, and dynamic security analysis identifies vulnerabilities in run-time behavior, while CATA identifies security issues in requirements, architecture, and high-level design.

CATA – Complementary Security Services: CATA is a high-level service focused on the requirements and architectural level. Problem areas identified through CATA can often be addressed through other Contractor security service offerings. The following additional services help assess whether the security designed in early stages is also implemented correctly:

- **Secure Code Analysis** – Provides validation that the application, once it has been designed correctly, is implemented as designed. This may be a combination of human expert security code review and automated static scanning, such as with HPE Fortify.

- **Applications Vulnerability Assessment** – Provides a further layer of validation that once the application is implemented as designed, known attack vectors do not “break” it. Vulnerability assessment can be performed not only prior to deployment, but also throughout the production lifetime of the application. The assessment can catch some emerging or “zero day” problems with applications that have already been deployed to the field.
- **Penetration Testing** – Penetrates beyond vulnerability assessment to test vulnerabilities discovered in vulnerability assessment for exploitability.

- Automated systems and tools involved in solution

HPE Fortify on Demand, CATA tools and templates, referenced above. Note that HPE Fortify is distinct from CATA, which analyzes analyses security requirements, architecture, and high-level design, and is human methodology, whereas Fortify is a product/tool to scan code statically (for instance Fortify SCA) and dynamically (WebInspect). These tools are highly complementary, and when used   in combination with human expert and hybrid Secure Code Analysis and application vulnerability assessment and penetration testing, they cover security across all major aspects of the SDLC.

10. CONTRACTOR TOOLS

Following is a list of the tools used in Contractor's solution to provide services to the County.

RESOURCE / TOOL NAME	INFORMATION
Enterprise System List (ESL)	Type: Software Manufacturer: HPES Purpose/Use: ESL (Enterprise System List) is a Delivery-focused Configuration Management System for managing System/Application Configuration Items, Services/Contracts and Customer/Account Information. Other Information: Supported Services: Configuration Management Services
Asset Manager	Type: Software Manufacturer: HPE Purpose/Use: Tracks End-User and network assets Other Information: Supported Services: Configuration Management Services, End User Services, Domain Name Management Services Supported Services: Cross Functional
Discovery and Dependency Mapping Inventory (DDMI)	Type: Software Manufacturer: HPE Purpose/Use: discovers and reports assets found on the network; integrates with Asset Manager. Other Information: Supported Services: Cross Functional
Service Manager (HPSM)	Type: Software Manufacturer: HPE Purpose/Use: Used by the Service Desk and all support staff for ticketing of Incidents, Problems and Changes. Other Information: Supported Services: Service Delivery Management, Incident Management, Problem Management Services, Change Management Services, Release Management Services, Service Desk Services, End User Services, Core Software Services, County Retained Assets Services, Catalog Services, Network Printer Services, Configuration Management Services
End User Access (EUA)	Type: Software Manufacturer: HPES Purpose/Use: Service Portal Other Information: While the core software and interfaces are standardized and centrally controlled to interact with the rest of the cross functional tools, the Service Portal is separately instantiated and customized for each client for whom it is deployed.

RESOURCE / TOOL NAME	INFORMATION
	Supported Services: Project Management Services, Reporting Management Services, County Retained Asset Services, Catalog Services, Application Maintenance and Operations Services
Aries/Aldea	Type: Software Manufacturer: HPES Purpose/Use: Tool used by Contractor internally to request resources (e.g., staffing assignments, workload placement) from the broader Contractor community Other Information: Supported Services: Cross Functional
RevGen	Type: Software Manufacturer: SAP Ariba Purpose/Use: Procurement of products and services Other Information: Supported Services: Cross Functional
Enabling Delivery and Global Excellence (EDGE)	Type: Knowledge Repository Manufacturer: HPES Purpose/Use: EDGE is a holistic environment that includes all the information needed to enable Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each of the ES business units by providing process artifacts that can be leveraged and used as part of their day-to-day work. Other Information: Supported Services: Architecture Services, Business Analyst Services, Project Management Services
Enterprise Architect	Type: Software Manufacturer: Sparx Systems Purpose/Use: Enterprise Architect provides full life cycle modeling for: Business and IT systems Software and Systems Engineering Real-time and embedded development Other Information: Supported Services: Architecture Services
ProVision	Type: Software Manufacturer: OpenText Purpose/Use: ProVision is Contractor’s standard modeling tool, to be used for Business Process, Enterprise Architecture and IT solution modeling. It enables business & IT teams to visually create models, describing business process, process interactions and detailed workflow Other Information: Supported Services: Architecture Services, Business Analyst Services*

RESOURCE / TOOL NAME	INFORMATION
Disaster Recovery Subscription Services	Type: Disaster Recovery Subscription Services Manufacturer: various Purpose/Use: DR subscription services for all leveraged hardware and software used to provide: Server services, Storage services, Network services, Security services and Backup services Other Information: Note that the Centera and the dedicated firewalls located in the DR site are not considered to be part of this list, since they are dedicated to the County. Supported Services: Cross Functional
ArcSight Security Information and Event Management (SIEM)	Type: Software/appliance Manufacturer: HPE Purpose/Use: Event logging and monitoring Other Information: Supported Services: Security Services
Global Delivery Capacity & Performance Management (GDCPM)	Type: Software Manufacturer: HPES (based on SAS and other underlying tools) Purpose/Use: Collects, aggregates and analyzes capacity and performance data from various disparate sources for reporting and analysis Other Information: Supported Services: Capacity Planning and Performance Management Services
System Center Configuration Manager (SCCM)	Type: Software Manufacturer: Microsoft Purpose/Use: Hardware discovery and software distribution to End-User devices Other Information: Security patching of OS and distribution of desktop software Supported Services: End User Services, Core Software Services, County Retained Assets Services, Catalog Services, Application Maintenance and Operations Services, Initiatives: User Data Services
Leveraged Internet Service (LIS) firewalls in the Tulsa and Colorado Springs data centers	Type: Hardware Manufacturer: Checkpoint Purpose/Use: Internet access/security Other Information: In the future these are slated to be replaced by Fortinet firewalls Supported Services: Network Services
AT&T Commonly Shared Network	Type: equipment, tools, software, systems and other materials Manufacturer: Various Purpose/Use: For clarity, the AT&T Commonly Shared Network means (i) the public or shared networks of AT&T, its Affiliates and their subcontractors, and the equipment, tools, technologies, systems, software, and other materials that are components thereof; (ii) equipment, tools, technologies, systems, software and other materials used by AT&T, its Affiliates and their subcontractors in shared network management and back office environments including ,

RESOURCE / TOOL NAME	INFORMATION
	without limitation, TIRKs, iGEMS, BusinessDirect, Billing Edge, the AT&T Global Network Client and AT&T Connect and any other items listed above in this Exhibit; and (iii) all modifications, upgrades, derivative works, enhancements, improvements and extensions of any of the foregoing. Other Information: Supported Services: Network Services
SIMS (Security Information Management System)	Type: Software Manufacturer: AT&T Purpose/Use: Security event correlation Other Information: Supported Services: Network Services
SDNOM (Software Defined Network Order Management)	Type: Software Manufacturer: AT&T Purpose/Use: Circuit Ordering Other Information: Supported Services: Network Services
Nectar Unified Communication Management Platform	Type: Software Manufacturer: Nectar Purpose/Use: Voice Network Performance Management Other Information: Supported Services: Network Services
MDM-Airwatch SaaS Console (Mobile Device Management)	Type: Software Manufacturer: AT&T Purpose/Use: Mobile device management Other Information: Offers a centralized dashboard to enforce policies, set restrictions, and secure devices while in use, lost, or stolen. Supported Services: End User Services, County Retained Assets Services, Mobility Infrastructure Services
SORD (Service Order Retrieval and Distribution)	Type: Software Manufacturer: AT&T Purpose/Use: Service order entry Other Information: Supported Services: Network Services
Telegence	Type: Software Manufacturer: AT&T Purpose/Use: Billing Other Information: Supported Services: Network Services
BOSS (Billing and Ordering Support System)	Type: Software Manufacturer: AT&T Purpose/Use: Product billing, tracking and reporting Other Information: Supported Services: Network Services

RESOURCE / TOOL NAME	INFORMATION
DPSS (Data Products and Services System)	Type: Software Manufacturer: AT&T Purpose/Use: Data product and services tracking Other Information: Supported Services: Network Services
BusinessDirect/eBill	Type: Software Manufacturer: AT&T Purpose/Use: Account management Other Information: Supported Services: Network Services
Exchange Plus	Type: Software Manufacturer: AT&T Purpose/Use: Carrier resource tracking Other Information: Supported Services: Network Services
ICES (Integrated Customer Enterprise System) ServiceCenter/AssetCenter	Type: Software Manufacturer: AT&T Purpose/Use: Asset Inventory Other Information: Supported Services: Network Services
SAINT	Type: Software Manufacturer: AT&T Purpose/Use: Security scanning and testing Other Information: Supported Services: Network Services
Nmap	Type: Software Manufacturer: Nmap Purpose/Use: Network scanning and mapping Other Information: Supported Services: Network Services
WFA (Work Force Administration)	Type: Software Manufacturer: Telcordia Purpose/Use: Trouble ticketing and work flow Other Information: Supported Services: Network Services
TIRKS (Trunks Integrated Record Keeping System)	Type: Software Manufacturer: Telecordia Purpose/Use: Circuit design Other Information: Supported Services: Network Services
AOTS-TM (AT&T One Ticketing System – Trouble Management)	Type: Software Manufacturer: AT&T/Remedy Purpose/Use: trouble ticketing Other Information:

RESOURCE / TOOL NAME	INFORMATION
	Supported Services: Network Services
NMA (Network Monitoring and Analysis)	Type: Software Manufacturer: Telecordia Purpose/Use: Network monitoring Other Information: Supported Services: Network Services
Avaya Site Administration	Type: Software Manufacturer: Avaya Purpose/Use: Voice system administration Other Information: Supported Services: Network Services
Server Automation	Type: Software Manufacturer: HPE Purpose/Use: Distributing operating system and layered product patches and upgrades Other Information: The core mesh is a shared resource; distribution satellite servers within the County's network zones are dedicated to the County Supported Services: Managed Private Cloud
Operations Manager (HPOM)	Type: Software Manufacturer: HPE Purpose/Use: Monitoring and alerting for various data center components, such as servers, domain controllers, databases, etc. Other Information: Supported Services: Managed Private Cloud, Application Maintenance and Operations Services
Microsoft Office 365 Government Community Cloud	Type: Software as a Service Manufacturer: Microsoft Purpose/Use: E-Mail (Exchange Online), Collaboration (SharePoint Online, Skype for Business), Cloud File Management (OneDrive for Business) Other Information: Supported Services: Data Center Services
E2E Complete	Supported Services: Transition Schedule and Tasks Type: Software Manufacturer: BinaryTree Purpose/Use: Automation tool for migration of mail services from Exchange to the Microsoft Office 365 Cloud Other Information: Supported Services: Unified Communications Infrastructure Services
Helion Virtual Private Cloud for US Public Sector	Type: Infrastructure as a Service Manufacturer: HPE Purpose/Use: Virtual Private Cloud (VPC) for Windows and Linux environments. VPC is a Government Community Cloud currently used to run the County's Beach and Water Quality website.

RESOURCE / TOOL NAME	INFORMATION
	Other Information: Data Center Services
Watchdog	Type: Software Manufacturer: HPES Purpose/Use: Internally developed utility that monitors/removes privileged access implemented via non-approved methods Other Information: Supported Services: Security Services
StarTeam	Type: Software Manufacturer: Microfocus/Borland Purpose/Use: Software Change and Configuration Management Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Applications M&O
Together	Type: Software Manufacturer: Microfocus/Borland Purpose/Use: Together enables software to be designed using industry-standard UML notation and conventions. With a large number of built-in utilities to manage the software design process, validate designs and generate code, together helps maximize the efficiency and accuracy of the software development process Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Business Analyst Services
Agile Manager	Type: Software Manufacturer: HPE Purpose/Use: Agile project management is a SaaS (software-as-a-service) solution that helps teams to organize, plan, and execute Agile projects. Other Information: This tool may also be used in Business Analysis and Applications M&O Other Information: Supported Services: Applications M&O
Team Foundation Server	Type: Software Manufacturer: Microsoft Purpose/Use: Microsoft Team Foundation Server (TFS) is a set of tools and technologies that enable a team to collaborate and coordinate the development and build efforts for a .NET software product or completing a .NET software project. Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Configuration Management Services
MEGA	Type: Software Manufacturer: Mega

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: to help enterprise architects and business stakeholders get a digital representation of their organization and its strategy, goals, business processes, and resources. Other Information: Supported Services: Architecture Services
Project and Portfolio Management (PPM)	Type: Software Manufacturer: HPE Purpose/Use: Project Management Integration, prioritization, demand management Other Information: SAAS Solution Supported Services: Architecture Services, Project Management Services, Business Analyst Services, Applications Maintenance and Operations Services
Apps (Applications) Manager	Type: Software Manufacturer: HPES Purpose/Use: to track and report on Portfolio Application information. Other Information: Supported Services: Architecture Services, Configuration Management Services
MS SharePoint	Type: Software Manufacturer: Microsoft Purpose/Use: Collaboration, Integration, Reporting and Workflow Other Information: Supported Services: Project Management, Reporting Management
myRequests	Type: Software Manufacturer: HPES Purpose/Use: Requests Management, Collaboration, Integration and Workflow Other Information: Supported Services: Project Management, Reporting Management
DocVault	Type: Software Manufacturer: HPES Purpose/Use: Collaboration and Document Storage Other Information: Custom Documentum and SharePoint Integration for storage of documentation Supported Services: Project Management, Reporting Management
Application Lifecycle Management (ALM)	Type: Software Manufacturer: HPE Purpose/Use: Quality Management, Testing Management and Measurement, functional testing. Manage test cases and test scripts and track test results Other Information: SAAS Solution Supported Services: Integration and Testing Services, Applications Development Services

RESOURCE / TOOL NAME	INFORMATION
Requirements Ambiguity Checker	Type: Software Manufacturer: HPE Purpose/Use: Requirements Validation Other Information: Supported Services: Integration and Testing Services
Performance Center	Type: Software Manufacturer: HPE Purpose/Use: Performance Testing Other Information: Supported Services: Integration and Testing Services
Unified Functional Tester	Type: Software Manufacturer: HPE Purpose/Use: Regression Testing Other Information: Supported Services: Integration and Testing Services
WebLogic Server 11gR1 Generic and Coherence	Type: Software Manufacturer: Oracle Purpose/Use: Middleware Other Information: Supported Services: Identity and Access Management Services
Identity Manager	Type: Software Manufacturer: Oracle Purpose/Use: Manage End-User access privileges Other Information: Supported Services: Identity and Access Management Services, Initiative: Identity Federated Services
Access Manager	Type: Software Manufacturer: Oracle Purpose/Use: Provides adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization extended to mobile clients and mobile applications. Other Information: Supported Services: Identity and Access Management Services, Initiative: Identity Federated Services
Fusion Middleware Repository Creation Utility 11g	Type: Software Manufacturer: Oracle Purpose/Use: Code Repository Other Information: Using SVN Supported Services: Identity and Access Management Services
Enterprise Content Management 11g	Type: Software Manufacturer: Oracle Purpose/Use: Content Management Other Information: Supported Services: Identity and Access Management Services

RESOURCE / TOOL NAME	INFORMATION
SQL Server Business Intelligence	Type: Software Manufacturer: Microsoft Purpose/Use: Creating SQL Queues and Reports Other Information: Supported Services: Reporting Management Services
MindMeister	Type: Software Manufacturer: Purpose/Use: Online mind mapping tool that enables users to capture, develop, and share ideas visually Other Information: Supported Services: Business Analyst Services*
Active Directory and Group Policy	Type: Software Manufacturer: Microsoft Purpose/Use: Used to manage the database of resources on the network Other Information: Microsoft environment printer management tools Supported Services: End User Services, Network Printer Services, Initiative: Identity Federated Services
Office Configuration Analyzer Tool (OffCAT)	Type: Software Manufacturer: Microsoft Purpose/Use: Provides a detailed report on installed Office programs and Highlights known problems Other Information: Supported Services: End User Services
Diagnostic Toolset	Type: Software Manufacturer: HPE Purpose/Use: Hardware diagnostics includes hard drive scanning repair, memory testing Other Information: Supported for Win7 and Win10 Supported Services: End User Services
Endpoint Protection / Encryption	Type: Software Manufacturer: Symantec Purpose/Use: Full disk and removable media encryption management. Anti-virus and anti-malware solution Other Information: Supported Services: End User Services, Core Software Services, Security Services
LogMeIn Rescue (LMI)	Type: Software Manufacturer: LogMeIn Purpose/Use: Provides secure remote control into End-User's device, to investigate and resolve issues Other Information: Supported Services: End User Services

RESOURCE / TOOL NAME	INFORMATION
Forcepoint Data Loss Prevention	Type: Software Manufacturer: WebSense Purpose/Use: Data loss protection on workstations Other Information: Supported Services: Core Software Services
Managed PKI	Type: Software Manufacturer: Symantec Purpose/Use: Device certificates for authentication Other Information: Supported Services: Core Software Services
Nessus	Type: Software Manufacturer: Tenable Network Security Purpose/Use: Vulnerability scans of workstations Other Information: Supported Services: Core Software Services, Security Services
Metasploit	Type: Software Manufacturer: Metasploit Purpose/Use: Validates that security of the core software configuration is acceptable prior to addition of new components to the configuration Other Information: Penetration Testing Supported Services: Core Software Services, Security Services
Expert Systems	Type: Software Manufacturer: Avaya Purpose/Use: Avaya maintenance services include Avaya Expert Systems and Secure Access Link (SAL). Avaya Expert Systems provides the County with Core Voice Services, a maintenance database of more than 30,000 artificial intelligence algorithms (AIAs) with scripted automation. These scripts automatically correct many known system- and software-related issues. Avaya SAL is a centralized consolidation point for all Avaya core systems for health and alarm monitoring, secure remote access using secure outbound-only HTTPS, and an integration point for Avaya Expert Systems. Other Information: Supported Services: Mobile Device Support Services, Voice Services, Initiative: Voice Services Transformation
Unified Communication Management Platform (UCMP)	Type: Software Manufacturer: Nectar Services Corp Purpose/Use: provides multivendor management services including application dependency, tree visual alerting, and vendor knowledge modules Other Information: Supported Services: Mobile Device Support Services, Voice Services, Initiative: Voice Services Transformation

RESOURCE / TOOL NAME	INFORMATION
CA eHealth	Type: Software Manufacturer: CA Technologies Purpose/Use: Performs capacity, performance, and trend analytics for circuits Other Information: Supported Services: Data Network Services, Video Conferencing Services, Wireless Network Access Services, Third-Party Network Access Services, IP Address Management Services
CA Spectrum	Type: Software Manufacturer: CA Technologies Purpose/Use: Monitors all network equipment—routers, switches, wireless access point (WAP) controllers, and WAPs—and provides alerts/alarms based on predefined parameters Other Information: Supported Services: Data Network Services, Remote Access Services, Video Conferencing Services, Wireless Network Access Services, Third-Party Network Access Services, IP Address Management Services, Initiatives: IT Application Portfolio Management Services
Cascade Shark	Type: Software Manufacturer: Riverbed Purpose/Use: Performs NetFlow data capture for subsequent troubleshooting and in-depth packet analysis by Cascade Pilot Other Information: Supported Services: Data Network Services, Application Maintenance and Operations Services*, Initiatives: IT Application Portfolio Management Services
Cascade Pilot	Type: Software Manufacturer: Riverbed Purpose/Use: Performs in-depth network packet analysis Other Information: Supported Services: Data Network Services
SMARTnet Total Care (SNTC)	Type: Software Manufacturer: Cisco Purpose/Use: Discovers and reports on all Cisco equipment and maintains the database of all Cisco equipment. Automates the process of gathering data for direct vendor support in the event of a problem. Other Information: Supported Services: Data Network Services, Initiatives: IT Application Portfolio Management Services
AirWave	Type: Software Manufacturer: Aruba Purpose/Use: Provides inventory and control of wireless access points and controllers Other Information: Supported Services: Data Network Services, Wireless Network Access Services

RESOURCE / TOOL NAME	INFORMATION
Prime Infrastructure	Type: Software Manufacturer: Cisco Purpose/Use: Provides Cisco equipment configuration management and control; backs up equipment configurations and manages licenses Other Information: Supported Services: Data Network Services, Wireless Network Access Services, Initiatives: IT Application Portfolio Management Services
Juniper JSA3800	Type: Software Manufacturer: Juniper Networks Purpose/Use: Collects logging information about all remote access connections and supports the routine review of the logs Other Information: Supported Services: Remote Access Services
Wireless Control System (WCS)	Type: Software Manufacturer: Cisco Purpose/Use: to measure and take action to maximize performance of the network, as well as to provide ongoing reporting. Other Information: Supported Services: Wireless Network Access Services
Luna Control Center	Type: Software Manufacturer: Akamai Purpose/Use: to perform the essential activities of external DNS support Other Information: Supported Services: External DNS Management Services
PAM Adonis and Proteus systems	Type: Software Manufacturer: BlueCat Networks Purpose/Use: to collectively fulfill all of the IPAM requirements and support adherence to the service level requirements Other Information: Supported Services: IP Address Management Services
MS Project	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services
MS Excel	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services

RESOURCE / TOOL NAME	INFORMATION
MS PowerPoint	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services
Exchange Online Protection	Type: Software Manufacturer: Microsoft Purpose/Use: Antivirus protections, Antispam filters, Policy enforcement, Graymail detection, safe-unsubscribe, Email based threats (phishing, targeted attacks), Outbreak filters, Data Loss Prevention, Email Encryption Other Information: Supported Services: Security Services
Controlled Compliance Suite (CCS)	Type: Software Manufacturer: Symantec Purpose/Use: Policy compliance for servers Other Information: Supported Services: Security Services
Enterprise Reporter	Type: Software Manufacturer: Dell Purpose/Use: Active Directory Reporting Other Information: Supported Services: Security Services
Recovery Manager AD	Type: Software Manufacturer: Dell Purpose/Use: Restore deleted or corrupted objects and domain or forest Other Information: Supported Services: Security Services
Cloud Service Automation	Type: Software Manufacturer: HPE Purpose/Use: Automation of cloud management and provisioning Other Information: Supported Services: Managed Private Cloud
Helion Managed Cloud Broker	Type: Software Manufacturer: HPE Purpose/Use: This tool is extendable to remote virtual environments and can integrate with public cloud vendors such as Amazon Web Services and Microsoft Azure Other Information: Supported Services: Managed Private Cloud
Operations Orchestration Server (OO)	Type: Software Manufacturer: HPE Purpose/Use: Process workflow automation Other Information:

RESOURCE / TOOL NAME	**INFORMATION**
	Supported Services: Managed Private Cloud
Operations Orchestration Remote Access Server	Type: Software Manufacturer: HPE Purpose/Use: Remote access to OO Other Information: Supported Services: Managed Private Cloud
v-Center	Type: Software Manufacturer: VMware Purpose/Use: Server virtualization management Other Information: Supported Services: Managed Private Cloud
Infoscale	Type: Software Manufacturer: Veritas Purpose/Use: Filesystem management and clustering in specific Solaris environments Other Information: Supported Services: Managed Private Cloud*
Storage Foundation	Type: Software Manufacturer: Symantec Purpose/Use: Filesystem management and clustering in specific Solaris environments Other Information: Supported Services: Managed Private Cloud*
SiteScope	Type: Software Manufacturer: HPE Purpose/Use: for monitoring application thresholds and events Other Information: Supported Services: Managed Private Cloud
Codar	Type: Software Manufacturer: HPE Purpose/Use: For version-controlled, one-click deployments, rollbacks and promotions Other Information: Supported Services: Development and Test Services, Application Development Services
3PAR System Utilities	Manufacturer: 3PAR Purpose/Use: 3PAR array-based replication allows background replication of storage from one array to another. 3PAR Storage Peer Motion is used to migrate storage data volumes without any interruption in accessing the data. Other Information: Supported Services: Storage Services, Storage Architecture Type: Software

RESOURCE / TOOL NAME	INFORMATION
BUR Dashboard	Type: Software Manufacturer: HPES Purpose/Use: This notifies BUR admins and End-Users of both successful and missed backups. It identifies for the BUR admins which nodes to work and automates BUR jobs Other Information: Supported Services: Backup and Recovery Services
Print Server	Type: Software Manufacturer: BARR Systems Purpose/Use: To automate and control print and document output Other Information: Supported Services: Managed Print Services
Symantec Management Console	Type: Software Manufacturer: Symantec Purpose/Use: to provision and revoke certificates and configure applications to use those certificates, reporting, and administrative End-User management services Other Information: Supported Services: Public Key Infrastructure Services
Applications Performance Management (APM)	Type: Software Manufacturer: HPE Purpose/Use: Provides a 360-degree view that verifies the performance of desktop, web, and mobile apps for on premise, cloud, or hybrid environments Other Information: Supported Services: Application Maintenance and Operations Services*
Toad	Type: Software Manufacturer: Dell Purpose/Use: For Oracle software Other Information: Supported Services: Application Development Services
PST Capture	Type: Software Manufacturer: Microsoft Purpose/Use: For searching and harvesting PST files Other Information: Supported Services: Transition Schedule and Tasks
DoubleTake	Type: Software Manufacturer: Vision Solutions Purpose/Use: a migration tool that performs a complete server copy from the source server onto the target server. Other Information: Supported Services: Consolidated and Single Data Center

RESOURCE / TOOL NAME	INFORMATION
PlateSpin	Type: Software Manufacturer: NetIQ Purpose/Use: Similar to DoubleTake, PlateSpin performs a complete server copy from the source server to the target server, if needed. It allows source servers to be copied as an image that can be transported using an approved portable storage device Other Information: Supported Services: Consolidated and Single Data Center
Panorama	Type: Software Manufacturer: Palo Alto Networks Purpose/Use: Provides a central repository for logging, inventory of the Palo Alto components, licensing management, software image management, and analysis Other Information: Supported Services: Initiatives: IT Application Portfolio Management Services
E911 Manager	Type: Software Manufacturer: Unknown Purpose/Use: Automates the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T MPLS network to track and update VoIP, digital, and analog phone moves, adds, and changes. Other Information: Supported Services: Initiative: Voice Services Transformation, Initiative: E911
E911 Anywhere	Type: Software Manufacturer: Unknown Purpose/Use: A cloud-based 911 call routing service that can connect a 911 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada. Other Information: Supported Services: Initiative: Voice Services Transformation, Initiative: E911
SPM	Type: Software Manufacturer: Unknown Purpose/Use: Unknown Other Information: Supported Services: Initiative: Storage Architecture
ControlPoint	Type: Software Manufacturer: HPE Purpose/Use: Analyzing unstructured data for cleaning up and archive Other Information: Supported Services: Initiative: Storage Architecture
SDM	Type: Software Manufacturer: HPE

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: To reduce the data footprint of structured data Other Information: Supported Services: Initiative: Storage Architecture
OneView	Type: Software Manufacturer: HPE Purpose/Use: Common software-defined convergence platform Other Information: Supported Services: Initiative: Storage Architecture
Federation Manager Identity Federation (OIF)	Type: Software Manufacturer: Oracle Purpose/Use: Provides secure identity information exchange between external/internal partners. OIF provides account management for partner identities and integrations. OIF integrates with a wide variety of data stores, End-User directories, authentication providers, and applications. Other Information: Supported Services: Initiative: Identity Federated Services
Virtual Directory, Unified Directory	Type: Software Manufacturer: Oracle Purpose/Use: Internet and industry-standard Lightweight Directory Access Protocol (LDAP) and eXtensible Markup Language (XML) views of existing enterprise identity information without synchronizing or moving data from its native locations. Other Information: Supported Services: Initiative: Identity Federated Services
Active Directory Federated Services (ADFS)	Type: Software Manufacturer: Microsoft Purpose/Use: Provide users with SSO access to systems and applications located across organizational boundaries. Other Information: Supported Services: Initiative: Identity Federated Services
Fortify on Demand	Type: Software Manufacturer: HPE Purpose/Use: To scan code statically Other Information: Supported Services: Other Proposed Initiative: Comprehensive Applications Threat Analysis (CATA) Service
Netcool	Type: Software Manufacturer: IBM Purpose/Use: Monitoring data center network devices Other Information: Supported Services: Network Services

RESOURCE / TOOL NAME	INFORMATION
Network Node Management Interface (NNMi)	Type: Software Manufacturer: HPE Purpose/Use: Monitoring performance/capacity of data center circuits and devices Other Information: Supported Services: Network Services
Wireshark	Type: Software Manufacturer: Wireshard Purpose/Use: such as for deep packet capture analysis Other Information: Supported Services: Network Services
Bluejeans	Type: Software Manufacturer: Bluejeans Purpose/Use: portal access to evaluate End-User and conference usage and detail Other Information: Supported Services: Video Conferencing Services
Enterprise Manager	Type: Software Manufacturer: Oracle Purpose/Use: to provide performance metrics, historical data, trending & reporting. Other Information: Supported Services: Supported Services: Video Conferencing Services
PVCS	Type: Software Manufacturer: Serena Purpose/Use: Archived project documents and application code Other Information: Supported Services: Supported Services: Applications Services, Project Management Services
AssetEdge Lease Manager	Type: Software Manufacturer: HPE Financial Services Purpose/Use: Lease tracking Other Information: Supported Services: Asset Management Services
PKI	Type: Software Manufacturer: Microsoft Purpose/Use: Certificate authentication Other Information: Supported Services: Security Services
Pretty Good Privacy (PGP)	Type: Software Manufacturer: Symantec Purpose/Use: File encryption Other Information: Supported Services: Security Services

RESOURCE / TOOL NAME	INFORMATION
StoreServ Management Console	Type: Software Manufacturer: HPE Purpose/Use: 3PAR management and reporting console for converged management of both File and Block on HPE 3PAR StoreServ Storage systems. Other Information: Supported Services: Storage Services, Storage Architecture
3PAR Command Line interface (3PAR CLI)	Type: Software Manufacturer: HPE Purpose/Use: To monitor, manage, and configure 3PAR storage Systems. Other Information: Supported Services: Storage Services, Storage Architecture

*Tool is listed as an option for use with this Service

11. County Applications by PA-ID

PAID	NAME
PA1002	AIS Master Mailing List
PA1005	AAB Labels
PA1008	ACAP/ACVV Values, Rates, Apportion
PA1014	Accounts Receivable and Trust
PA1017	ACRC Roll Corrections Process
PA1018	ACST/TC Auditor Secured Tax Billing
PA1019	ACTI Tax Rate Area Index
PA1020	ACUS Auditor Unsecured Prpty Tax Billing
PA1024	Agricultural Preserves
PA1044	ASAD Secured Prpty Assess Info System
PA1045	ASAS Secured Prpty Assess Ownership&Valu
PA1046	ASPA Supplemental Property System
PA1047	ASRC Roll Corrections Process
PA1048	Assessment Appeals Board System
PA1049	ARCC Intranet Applications
PA1050	ARCC Internet Applications
PA1054	Audit Assignment Tracking
PA1058	AutoCAD
PA1073	CDS Online
PA1074	CDS Batch
PA1077	Ballot Enclosure Scanning System
PA1136	Chameleon
PA1158	Community Enhancement / Neighborhood Reinvestment Program (AC Grant)
PA1159	iVOS
PA1160	Comparable Sales System
PA1162	Computer Assisted Mass Appraisal (CAMA)
PA1174	County Law
PA1179	Criminal Case Tracking-JURIS
PA1187	Cut Log Tracking

PAID	NAME
PA1188	County Intranet Site
PA1196	CME Web
PA1202	DHR Internet Class/Comp info.
PA1247	Field Survey Notes Index
PA1270	Geo-Coding System
PA1308	TTC Sonant IVR, ACD and Phone Payment System
PA1310	Homeowner Exemptions - AS/400
PA1313	IBM - Probation Records
PA1314	IDX Managed Care Application
PA1324	Interest Apportionment
PA1376	Traffic/Minor Offense Mainframe
PA1389	MPR Online
PA1409	Officer Notification System
PA1433	PAR File Online
PA1438	Precinct Activity Tracking System
PA1451	Performance Reports
PA1516	Prop 60/90/110
PA1517	Prop 8
PA1523	TTC Tax Sale Database
PA1564	Records Index
PA1566	Redemption (Prior Year/Secured/Defaulted) Taxes
PA1568	DPW Referrals System
PA1580	Restraining Order System
PA1588	RSVP Volunteer Reporter
PA1595	Sale of Data
PA1603	Section 11 Properties
PA1609	Sheriff ID
PA1610	Sheriff Licensing
PA1611	Sheriff Registrants
PA1643	Supplemental Online
PA1659	Timeshare Ownership Tracking
PA1665	Criminal History Tracking System

PAID	NAME
PA1680	TTC TRDS Defaulted Secured Data Mgmt (Mainframe)
PA1682	TTC TRST Tax Collector Secured Tax Collect (Mainframe)
PA1683	TTC TRTC Carryover (Mainframe)
PA1684	TTC TRTH Secured Tax History Info System (Mainframe)
PA1742	TTC TRRT Unsecured Tax Refund Mgmt System (Mainframe)
PA1745	TTC TRUS Unsecured Property Tax System (Mainframe)
PA1755	Volunteer Tracking System Polinsky
PA1759	Want/Warrant System
PA1766	Weather Monitoring and Flood Warning System
PA1782	Adoptions Assistance Program
PA1785	Animal Control - Lost and Found
PA1788	Autocad
PA1789	AutoLISP Files
PA1802	TTC TRCC Cortac (Mainframe)
PA1809	CWS/CMS Data Mart
PA1813	TTC Tax Sale Maps and Images (Web)
PA1814	DHR Internet Web Page
PA1820	EMISSIONS INVENTORY (EASIER)
PA1846	Natality Extract for Dr. Dobkins, UCSD
PA1855	Phone Directory (INTRANET)
PA1856	Precinct District Voter Counts
PA1857	Preliminary Notices
PA1865	Property Tax Characteristics
PA1869	Rasscle
PA1871	Recorder Vital Records System
PA1872	Red Envelope
PA1887	SIMWIN
PA1893	Tax Rate by Tax Rate Area Search
PA1900	Tran Control Log: Shrink Wrap

PAID	NAME
PA1901	Traverse
PA1902	ARCCs AX/WX/WFM Applications
PA1905	Web Polling Place Lookup
PA1907	Kinnosa
PA1917	Chargeback System
PA1920	Sales/Deposit Permit System
PA1921	SSRS
PA1922	Training Tracking
PA1923	Countywide Customer Satisfaction Survey
PA1927	Polinsky Donor Tracking System
PA1928	EZ Access
PA1933	ARCC E-Commerce
PA1940	CMIPS Adhoc Tool
PA1971	SUN (San Diego User Network)
PA1973	ISCP - CODE 1 Plus
PA1974	ISFC - FOCUS Front-End Processing
PA1976	ISTB - Telephone Billing
PA2005	County Web Mapping Applications
PA2012	Q-Matic Line Queue Management
PA2031	Juvenile Traffic
PA2044	Public Defender Intranet (PD)
PA2056	Edgemore Nurse Staffing program
PA2057	EZ Access Interfacing Systems
PA2060	PeopleSoft HCM
PA2065	Polinsky Kids Information Data System
PA2068	Administrative Investigations Management
PA2078	TTC Mobile Home Tax Clearance Database
PA2079	Parent/Child Property Transfer System
PA2081	Property Parcel Corrections Database
PA2082	ARCC Document Management System
PA2083	Certificate Signature Printing System
PA2089	Marshall-Swift Commercial/Agricultural Estimator

PAID	NAME
PA2090	MLS
PA2093	Integrated Report Systems (I.R.S.)
PA2094	Outside Purchase Control System (OPTICS)
PA2100	EZ Access – Jwalk
PA2102	Jail Information Management System Interfaces
PA2103	JCATS Criminal Case Management System
PA2110	Vital Records Information System
PA2113	Public Health Information System
PA2115	Banknote Paper Tracking
PA2127	Prof Photocopiers
PA2134	Survey Records Imaging System
PA2135	HR Employment Document Management System
PA2144	SPS Cut
PA2150	ERP Oracle Financials
PA2152	Business Audit Tracking
PA2153	Fraud Referral Tracking System
PA2154	Secure Web Drop Box
PA2156	Bar Code File Tracking System
PA2171	NTTData Netsolutions
PA2175	SOCAT
PA2186	Elite
PA2190	SPSS
PA2191	QANET Collector System
PA2193	TTC ApplicationXtender & WebXtender
PA2200	Child Health and Disability Program/Children Youth and Families/Health Care Program for Children in Foster Care
PA2201	TTC Wausau ImageRPS
PA2202	Sharpe IPM
PA2210	Workflow Manager for Revenue and Recovery Remittance System
PA2211	ERMXtender for ARCC
PA2215	Utility Manager Pro

PAID	NAME
PA2224	Volunteer Tracking System AIS
PA2233	DIMSNET
PA2235	Probation Case Management System
PA2237	ARCC Cashiering
PA2238	Innovative Millennium
PA2239	Special Assessments by Parcel Number Search
PA2242	Buynet II
PA2245	Kronos Workforce Central
PA2250	AXAddOns
PA2257	Source Test Tracking
PA2260	Hansen for Parks & Rec
PA2261	QBIS Data Recording System (DRS)
PA2262	San Diego Immunization Registry
PA2263	OneStep Database
PA2264	Mystery Shopper
PA2265	HHSA Program Guides
PA2267	WebTrends
PA2270	External Agencies WEB Reporting
PA2273	LUEG Repository
PA2286	TTC Trustref (TTC Financial Apps)
PA2287	Viking Data Entry System
PA2288	ARCC Recording System
PA2289	ARCC Mills Act DB
PA2293	Manual Clearing Database
PA2295	Purchasing and Contracting Documentum Repository
PA2300	TTC WARP (Wire Access Request Portal)
PA2308	PHIX
PA2309	AutoCAD Raster Design
PA2313	Columbia Ultimate RPCS
PA2314	Grant or Community Enhancement
PA2315	Medical Therapy Unit Online

PAID	NAME
PA2318	ROP Mobile Home DB
PA2319	Rental Mobile Home DB
PA2324	Kofax Ascent Capture 7.0
PA2337	Case Review System
PA2340	SDE Repository
PA2341	File Tracking System
PA2343	Closed Cases Repayment Accting System
PA2344	Cal Win Interfaces
PA2351	BOS District One Website
PA2352	BOS District Two Website
PA2353	BOS District Three Website
PA2354	BOS District Four Website
PA2355	BOS District Five Website
PA2356	Applications Manager
PA2357	Accela Automation (BCMS) (LEAMS)
PA2358	COB Public Search
PA2360	PCC Staffing Database
PA2361	myRequests
PA2369	Parent Search db
PA2371	Case Folder Tracking
PA2378	WITS
PA2385	CMS Patient Eligibility System
PA2391	MaxCars
PA2397	PatternStream
PA2399	Property Profile Mapping
PA2407	Food Facility Inspection Search
PA2413	County Web Referrals
PA2415	CCS Web Referrals
PA2417	CalWIN CIS Data Mart
PA2422	Proscript
PA2427	Absentee Voter Lookup
PA2429	ArborPro Management System

PAID	NAME
PA2430	NeoGov
PA2432	Northpointe COMPAS
PA2434	Kofax Ascent Capture – FG
PA2438	TTC WITS (Web Integrated Tax System)
PA2439	APS Imaging
PA2444	Citizen Advisory Boards Application
PA2445	Cerner Millennium
PA2446	Pharmacy Outpatient System (Etreby)
PA2447	Budget Books
PA2449	QCS AdHoc Statistical Reporting Subsystem
PA2455	HR Documentum
PA2456	CWS Mandated Reporter
PA2458	Prodagio
PA2459	ERP Data Archive
PA2461	TTC CRS (Central Reporting System)
PA2462	Card Access System
PA2468	AIS Ombudsman
PA2469	AIS Case Management
PA2470	StarLIMS – Web
PA2471	BMC Footprints
PA2477	TB – Fujifilm
PA2478	TTC Bloomberg Gateway
PA2479	HHSA HR Kofax Imaging
PA2480	HHSA AIS Ombudsman Kofax Imaging
PA2481	HHSA AIS APS Kofax Imaging
PA2482	HHSA AIS Case Management Kofax Imaging
PA2483	ARCC Q-MATIC Orchestra
PA2484	ARCC Captiva Scanning Solution
PA2485	AIS-IHSS Kofax Imaging
PA2486	AIS - IHSS Documentum/Webtop
PA2489	iQCS
PA2490	Electronic Approval Workflow

PAID	NAME
PA2491	CATS Customer Dashboard
PA2492	CRM Framework
PA2493	Integrated Recording & Vital Records System (aka. ACCLAIM)
PA2494	Medical Standards In-service Tracking
PA2495	AtPac Asset Manager
PA2496	Convey 1099
PA2499	TTC iPayment Cashiering
PA2501	DCSS Data Warehouse
PA2505	Inventory and Resource Management System
PA2507	Actuate BIRT 11
PA2509	ERP Oracle Data Warehouse
PA2510	PA Enrollment
PA2511	DGS Generic Filing Cabinet
PA2512	Public Authority Payroll History
PA2514	Documentum Import Tool
PA2515	PARTS - Public Authority Registry Tracking System
PA2518	Oracle Identity Manager
PA2519	ALEX (not an acronym)
PA2520	CalWin Case Comments
PA2524	Performance Budgeting
PA2525	AuditExchange
PA2527	TTC SharePoint iTTC
PA2530	ApprMapr - Web mapping application
PA2532	Justice Electronic Library System
PA2533	Community Resource Directory
PA2534	Oracle Fusion Middleware
PA2535	TTC Ad-Hoc Bill Printing
PA2536	Care Transitions Coach System
PA2538	Public Defender eShare
PA2540	Documentum Records Manager
PA2541	Building Automation System

PAID	NAME
PA2542	ARCC SharePoint Site
PA2543	P-Card Access Database
PA2544	PCMS To HHSA Interface
PA2546	County Constituent Relationship Management
PA2548	CobbleStone Data Synchronization
PA2549	IPTS-GRM
PA2557	Crossroads Software Collision Database System
PA2558	Identity and Access Management
PA2561	Cerner CareTracker
PA2562	CalWIN ERMS
PA2563	Enterprise Document Processing Platform
PA2567	San Diego Regional Resiliency Checkup
PA2569	ROV Documentum Generic File Cabinet
PA2571	Nicus M-PWR
PA2572	Client Visit Management
PA2573	Web Application for Legacy Payroll Data and Reports
PA2574	Pyxis
PA2575	Beach and Water Quality (BWQ)
PA2576	DCSS Business Intelligence - Tableau
PA2578	County Internet Website (AEM)
PA2580	LAFCO ApplicationXtender (AX) Imaging Environment
PA2581	TTC Interactive Web Response (IWR)
PA2582	GIS Mobile Applications
PA2583	CAR
PA2584	AP Invoice Imaging System
PA2586	Enterprise Email Solution
PA2587	A&C Captiva Scanning
PA2588	PCMS Knowledge Center
PA2589	PCMS Biometrics
PA2590	DocVault

PAID	NAME
PA2592	TempTrak
PA2593	DHR Document Repository for Medical Standards
PA2594	Probation Electronic Medical Records System (PEMR)
PA2595	Granicus - Citizen Participation Suite
PA2597	SharePoint 2013 Platform
PA2598	LiveWellSD.org
PA2599	Adobe e-Forms DEH Inspections
PA2600	TTC SeeTrans
PA2601	TTC EPS Express Manager
PA2602	EPI HIE SFTP Access
PA2603	DHR Captiva7 Scanning
PA2604	Probation Contact Log Mobile Application (PUMA)
PA2605	Transform for CalWIN Checks/Warrants
PA2606	DHR Documents upload to Documentum
PA2607	Bad Check Database
PA2608	Balance Due Report DB
PA2609	eForms Repository
PA2611	CoSign Digital Signature
PA2613	TTC AEM Internet Site (SDTREASTAX.COM)
PA2614	Information Exchange Program (ConnectWellSD)
PA2615	ROV AEM Website (SDVOTE.COM)
PA2617	Probation Work Projects
PA2618	DHR BENEFITS ELECTRONIC DOCUMENTS UPLOAD
PA2619	Selectron IVR
PA2620	Facil
PA2621	Alzheimer's Project AEM Website (SDAlzheimersProject.org)
PA2622	SDPARKS AEM Website (www.sdparks.org)
PA2629	Adobe e-Forms APCD Inspections

--- End of Document ---