Schedule 4.3 — Operational Services

Table of Contents

1. OVERVIEW OF SERVICES

1.1. Overview

This section describes the Services to be provided by the Contractor in various Service Frameworks, collectively also described herein as the Statement of Work (SOW). The objectives and requirements described in this Section 1 "Overview of Services" shall apply to all Service Frameworks without exception.

Capitalized terms used herein shall have the meaning assigned to them in Schedule A (Defined Terms) to the Agreement unless otherwise expressly defined in this Schedule.

1.2. High Level Requirements

1.2.1. Contractor shall provide Services to the County with a high level of quality and performance that meet or exceed the Service Levels.

1.2.2. Contractor shall provide equal or better service on all Service Frameworks in highest performance, capacity, and functionality as provided by the Legacy Provider.

1.2.3. Contractor shall provide continuous improvement to increase efficiency and effectiveness of County IT and Telecommunications Services over the life of the Agreement.

1.2.4. Contractor shall provide the technology expertise and resources required to provide Services in the most efficient and effective manner to meet the County's requirements.

1.2.5. Contractor shall provide strategies on emerging technologies that improve the County business operations and processes.

1.2.6. Contractor shall participate in, and support, the County's retained authorities in architecture, technology planning and standards establishment.

1.2.7. Contractor shall acquire and implement Services with availability guarantees that meet or exceed the defined Service Levels.

1.2.8. Contractor shall provide Services that can leverage operational scale and best practices to achieve optimum County price performance.

1.2.9. Contactor shall provide an annual report on improvements made since the previous report and improvements planned in the next year.

1.2.10. Contractor shall provide continuous improvement in Service Levels and provide a plan annually for improvements to Service Levels.

1.2.11. Contractor shall perform technology refresh and maintain technical currency that exceed or meet requirements.

1.2.12. Contractor shall acquire ongoing feedback mechanisms to ensure performance meets expectations.

1.2.13. Contractor shall maintain compliance with industry standards (e.g., ITIL) and government regulations.

1.2.14. Contractor shall maintain a customer focus and customer satisfaction while providing Services that are measurable and includes continuous improvement.

1.3. Environment

1.3.1. Tiers of Support

1.3.1.1. Contractor shall provide the up to five (5) tiers of support to End-Users.

1.3.1.2. Contractor shall provide all Tiers of Support 24/7/365.

1.3.1.3. Contractor shall continuously improve Tier 0 for End-User self-service.

1.3.1.4. Contractor shall continuously improve the performance and increase the knowledge at Tier 1 to resolve more End-Users Incidents at first call.

1.3.1.5. Defined Tiers of Support:

1.3.1.5.1. Tier 0

Tier 0 is the continuous updating and posting on the Service Portal of automated or self-service solutions, documents, instructions, videos, FAQs and like material that County End-Users can access without the aid of the Service Desk or Contractor Personnel.

1.3.1.5.2. Tier 1

Tier 1 are Service Desk calls that can provide basic support and troubleshooting, such as password resets, printer configurations, break-fix instructions, Incident routing and escalation to Tier 2 and Tier 3 support for End-Users. May also escalate to applications support or call for outside Third-Party maintenance (Tier 4), as needed.

1.3.1.5.3. Tier 2

Tier 2 support involves technical knowledge by more experienced technicians who have strong exposure to troubleshooting and handles break-fix, configuration issues, troubleshooting, software installations, and hardware. Tier 2 handles escalated Incidents from Tier 1. Tier 2 shall escalate unresolved Incidents to Tier 3 or to Tier 4.

1.3.1.5.4. Tier 3

Tier 3 is a very specialized job provided by the specialists who are usually involved in the product development and are capable of handling complex Incidents.

1.3.1.5.5. Tier 4

Tier 4 refers to Third-Party support, outside the County or Contractor. Escalation to Tier 4 support is for Incident resolution. This usually involves hardware and software Third-Party support for Portfolio Applications as an example.

1.3.2. Hardware and Software

Contractor shall provide all Hardware, Software, tools and knowledge databases used in the delivery of Services for each Service Framework. Contractor shall provision, install, manage, maintain, and support these Assets.

1.3.3. Facilities

1.3.3.1. County

All County Locations are within scope of the Agreement.

1.3.3.2. Contractor

All Locations utilized by the Contractor to provide the Services shall be provided, maintained, provisioned, and managed by the Contractor.

1.3.4. Personnel

Contractor shall be responsible for providing staff resources with the skills, qualifications, and experience to perform the Services in a high quality manner and to meet or exceed all Service Levels. Contractor's Account Executive, Contract Manager and two selected Key Personnel shall reside at the County Administration Center. A listing of Contractor Personnel to reside at various County Locations is to be developed and included in the final Transition Plan.

1.3.5. Policies, Procedures and Standards

Contractor shall be responsible for complying with all of the County's policies, procedures, and standards, including the Standards and Procedures Manual.

1.3.6. Agreements and Licenses

Contractor shall be responsible for the acquisition, management, and support of all agreements and licenses required for the Services.

1.3.7. Required Language(s)

English is the current required language. Contractor shall ensure that the level of English communications by all Contractor resources is sufficient to (i) be understandable by County staff and (ii) understand County staff.

1.4. Service Requirements

The descriptions of Operational Services in this Schedule follow the hierarchy of objectives and requirements:

1.4.1. This Overview of Services provides high-level requirements that apply to all of the Service Frameworks.

1.4.2. Each individual Service Framework includes a summary section describing requirements that apply to all of the Framework Components within the given Service Framework.

1.4.3. Each Framework Component includes requirements that apply specifically to the Framework Component, except for the Cross Functional Service Framework.

1.4.4. The Cross Functional Service Framework Components include requirements that apply to all Service Frameworks and Framework Components.

1.4.5. The Service Levels, referenced in Schedule 4.8, contain descriptions of Service Level requirements that apply across all the Service Frameworks.

1.4.6. Within each section, tables describing Roles and Responsibilities are included. These tables depict the County's Plan, Build, and Operate structure.

1.4.7. Service requirements in this Section use the structure depicted below:

Overview of Services

- Overview
- High Level Requirements
- Environment
- Service Requirements

These apply to all Service Frameworks and Framework Components

Service Frameworks

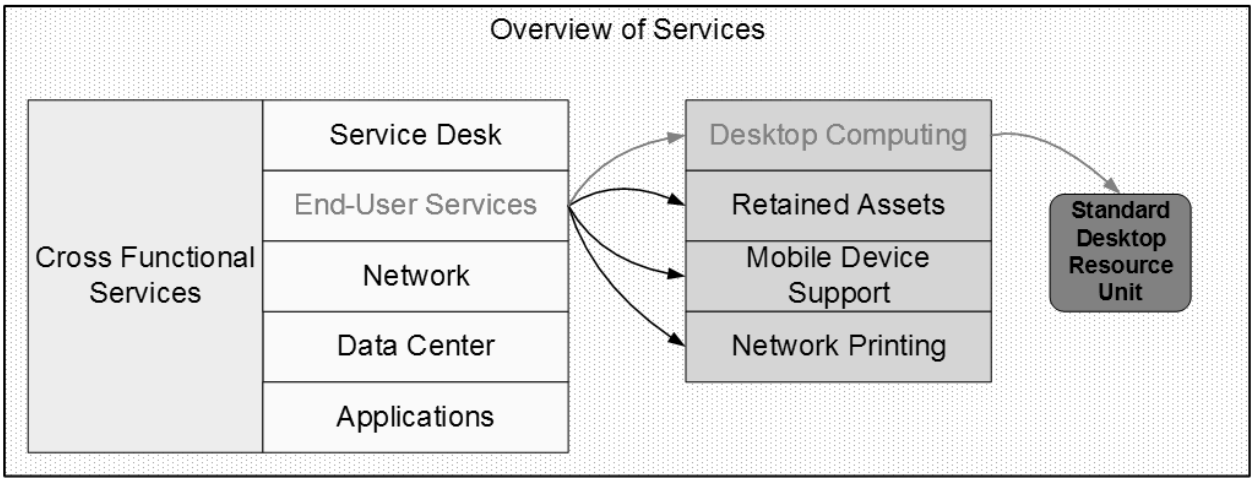
- Overview
- High Level Requirements
- Environment
- Roles and Responsibilities
  - Plan
  - Build
  - Operate

These apply to all the Framework Components within the specific Service Framework

Framework Components

- Overview
- High Level Requirements
- Environment
- Roles and Responsibilities
  - Plan
  - Build
  - Operate

These correspond to specific Resource Units



2. CROSS FUNCTIONAL SERVICES

2.1. Overview

This section pertains to the Cross Functional Services Framework. Cross Functional Services consist of the Plan, Build and Operate Services that spans across all Service Frameworks.

Cross Functional Services are composed of the following Framework Components:

- Contract and Acquisition Management Services
- Integrated Asset Management Services
- Billing Management Services
- Security Management Services
- Service Delivery Management (SDM) Services
- Architecture Services
- Project Management Services
- Integration and Testing Services
- Incident Management Services
- Problem Management Services
- Change Management Services
- Release Management Services
- Configuration Management Services
- Capacity Planning and Performance Management Services
- Disaster Recovery Services
- Identity Access Management Services
- Reporting Management Services
- Domain Names Management Services
- Business Analyst Services

Cross Functional Services include lifecycle services that Contractor shall provide across the County Service Frameworks. All requirements, roles and responsibilities described in Cross Functional Services considered to be within the scope for each Service Framework.

2.2. High Level Requirements

2.2.1. Contractor shall provide all Cross Functional Services Framework Components across each Service Framework.

2.2.2. Contractor shall recommend, for County approval, qualified Cross Functional Service Manager as Contractor Key Personnel to ensure delivery and quality of Cross Functional Services.

2.2.3. Contractor shall implement industry leading practices, process, quality, and project methodologies to align processes to people and technology to provide the Services.

2.2.4. Contractor shall develop and submit during Transition, management plans for each Cross Functional Services Framework Component to be included in the Standards and Procedures Manual.

2.2.5. Contractor shall continuously update and submit Cross Functional Services Framework Component management plans, for County approval, and include in the Standards and Procedures Manual.

2.2.6. Contractor shall continuously improve Cross Functional Services by monitoring trends and service quality improvement through independent research and recommending changes annually that improve efficiencies and reduce overall costs.

2.2.7. Contractor shall provide the County with insight into future direction, initiatives, and technology road maps of Third-Parties performing Cross Functional Services.

2.2.8. Contractor shall provide County with Applications, Software and business experience and expertise to support continuous improvement to Cross Functional Services.

2.2.9. Contractor shall provide inventory management across all Cross Functional Services Framework Components to ensure accurate counts, information, consolidated views, etc.

2.3. Contract and Acquisition Management Services

2.3.1. Overview

This section pertains to the Contract and Acquisition Management Services of the Cross Functional Framework. Contract and Acquisition Management Services are the roles and responsibilities for the management of the Agreement, Contractor's relationship with the County and to provide acquisition services.

Contractor's primary responsibilities under Contract and Acquisition Management Services are to:

- Serve as the single point of contact to work with the County to manage the Agreement and all related contracts to provide Operational Services, including disputes, amendments, communications and training.
- Execute and manage the Optional Items Catalog, licenses/support maintenance renewals, subscription renewals, perpetual license renewals, Cloud ASP renewals, Hardware maintenance, Software as a Service (SaaS) renewal, competitively procured Applications Development projects among Contractor sub-contractors and partners.
- Execute Third-Party procurements and market scan / procurement activities.

2.3.2. High Level Requirements

2.3.2.1. Contractor shall provide continuous improvement of Contract and Acquisition Management Services.

2.3.2.2. Contractor shall assign a full-time Contract Manager to act as the single point of contact for the County on all contractual matters, including subcontract(s). The Contract Manager shall cooperatively, promptly and continuously communicate with County-designated staff.

2.3.2.3. Contractor shall deliver quality, high and prompt response Contract Management Services to the County.

2.3.2.4. Contractor shall be responsive and work cooperatively with the County to address requests and resolve issues and disputes.

2.3.2.5. Contractor shall continuously assess the Agreement and recommend improvements to enable the continuous improvement delivery of the Services, with focus on optimizing County's operational performance.

2.3.2.6. Contractor shall work cooperatively to efficiently implement changes to the Agreement.

2.3.2.7. Contractor shall perform procurement activities to support and provide Services and respond to Service Requests (e.g., DAD, OIC, contracts, licenses, etc.).

2.3.2.8. Contractor shall negotiate and enter into contracts with the Third-Parties (except for situations where the Contractor and County agree in advance that the Contract shall be between the County and the Third-Party) upon County approval.

2.3.2.9. Contractor shall create, maintain and post on the Service Portal an accurate inventory of current contracts, procured services, County owner, purchases and other relevant key information that is readily accessible for validation, certifications, reviews and tracking.

2.3.2.10. Contractor shall manage the service catalog (e.g., Third-Party service contracts).

2.3.2.11. Contractor shall maintain a log of all and any purchases with information to track the requesting information to the End-User.

2.3.2.12. Contractor shall provide early notifications to the County point of contact(s) or County department for renewals.

2.3.2.13. Contractor shall manage license, subscriptions, maintenance, certifications agreements to ensure contract and County policy compliance.

2.3.2.14. Contractor shall provide County with requested support for County operational and financial planning information.

2.3.2.15. Contractor shall develop and document in the Standards and Procedures Manual a competitive procurement process that aligns with County competition procedures as outlined below:

- Board of Supervisors Policies A-87 – Competitive Procurement
- Policy A-97 – Protest Procedures for Award of Contracts
- B-39a – Veteran Owned Business (VOB) and Disabled Veterans Business Enterprise (DVBE) Program
- B-53 – Small Business Policy (SBP)

2.3.2.16. Contractor shall solicit market scans and proposals to respond to County-established business requirements and evaluation criteria, and participate with the County in the evaluation against the County-established business requirements and evaluation criteria (including associated integration requirements, if necessary) and shall enter into a contract with the selected Third-Party at the County's direction.

2.3.2.17. Contractor shall provide the County with assessments and recommendations for procurements of services in the cloud, including:

- Develop entry and exit criteria for any engagement with a Third-Party prior to contract signing that identify risks, portability, integration points and relevant impacts
- Develop and provide as part of any solution or procurement one-time and recurring costs, the associated contract terms, Service Levels, liability, insurance and related contract and legal information.
- Ensure the Third-Party meets County policies, regulatory requirements and mandatory requirements

2.3.2.18. Contractor shall create a section in the Standards and Procedures Manual for Contract and Acquisition Management activities and procedures including the procedures that link Contract and

Acquisition Management Services with, Service Desk Services, Applications M&O Services, and Applications Development.

2.3.2.19. Contractor shall annually update and deliver the Contract and Acquisition Management Services Management plan, for County approval, and post on the Service Portal.

2.3.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Contract and Acquisition Management Services.

Contract and Acquisition Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Contract and Acquisition Management policies and procedures.	X	
2. Review and approve Contract and Acquisition Management policies and procedures.		X
3. Produce and submit an overall performance measurement plan to complement the Service Levels. The performance measurement plan shall collect key metrics to enable the County and the Contractor to identify productivity gains, better manage the Services, and provide information for continuous improvement.	X	
4. Review and approve performance measurement plan.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Implement Contract and Acquisition Management policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
6. Support Contract and Acquisition Management policies and procedures with necessary staff and resources.	X	
7. Produce and submit a weekly and monthly program status report.	X	
8. Conduct monthly program status reviews with the County including status on the Contractor's achievement of the contractual objectives, specific issues with recommended solutions, and planned activities, and to receive feedback.	X	

Contract and Acquisition Management Roles and Responsibilities		
9. Produce and submit descriptions of contract issues and/or recommended contract PRR on as-needed basis.	X	
10. Review and approve contract PRR.		X
11. Provide program performance metrics to designated County staff members via Service Portal.	X	
12. Provide the County with weekly status updates to apprise relevant parties on the status of backlogged Service Requests and expected resolution dates.	X	
13. Manage relationship contact points with Third-Parties to deliver a single point of contact for the processing and resolution of issues and problems.	X	
14. Assist the County in developing and executing routine reports that allow insight into costs associated with the Agreement.	X	
15. Assist the County in the development of its annual budget by providing: • Current, detailed, and accurate information relating to past operations • Assistance in costing and balancing the implementation of major initiatives • Assistance in spreading the costs of these major initiatives over multiple budget cycles as appropriate • Technical support to determine the impact of changes in technology on costs. • Analysis of usage (i.e., volumes of Resource Unit consumption) and performance • Identification of technical solutions for the reduction of operational costs	X	
16. Produce and submit updates to the County Standards and Procedures Manual.	X	
17. Review and approve updates to the County Standards and Procedures Manual.		X
18. Conduct annual review of existing Third-Party agreements (including cloud applications) to ensure that the County is receiving optimal value from such agreements.	X	

Contract and Acquisition Management Roles and Responsibilities		
19. Review and approve the annual review of existing Third-Party agreements to ensure that the County is receiving optimal value from such agreements.		X

2.4. Integrated Asset Management Services

2.4.1. Overview

This section pertains to the Integrated Asset Management Services Framework Component of the Cross Functional Framework. The Integrated Asset Management Services are the activities and processes associated with tracking, managing, optimizing and continuously improving the overall control and inventory of Assets. Integrated Asset Management Services provides the capabilities to centrally manage all Asset repositories and report across all Assets. Integrated Asset Management Services enable an accounting of all Asset costs, to support strategy, architecture, funding and sourcing decisions.

2.4.2. High Level Requirements

2.4.2.1. Contractor shall acquire and provision all Assets required to perform the Services.

2.4.2.2. Contractor shall provide a County approved Integrated Asset Management System.

2.4.2.3. Contractor shall provide an Integrated Asset Management System that provides centralized management of all integrated Asset repositories including, but not limited to, inventory, financial and contractual data.

2.4.2.4. Contractor shall list ownership of all Assets (e.g., Contractor, County, and Third-Party) in the Integrated Asset Management System.

2.4.2.5. Contractor shall design and deliver an auto-discovery function for all Assets.

2.4.2.6. Contractor shall provide accessibility and search-ability by County for all Integrated Asset Management data.

2.4.2.7. Contractor shall provide monthly reports on all Assets.

2.4.2.8. Contractor shall effectively manage Assets from requisition to retirement.

2.4.2.9. Contractor shall continuously analyze, optimize and leverage County Asset licensing to ensure that the County is in compliance with all license requirements and also that the County is using the most economical number and distribution of licenses.

2.4.2.10. Contractor shall continuously analyze and optimize County maintenance and support agreements to ensure that the County has adequate maintenance and support.

2.4.2.11. Contractor shall identify any unnecessary maintenance and support agreements and promptly terminated.

2.4.2.12. Contractor shall ensure inventory of all Assets are maintained and accurate.

2.4.2.13. Contractor shall provide Integrated Asset Management System reports including Hardware, Software (Desktop Applications Directory and Applications Portfolio) License Compliance, Application and Infrastructure Servers and Personal Computing Assets.

2.4.2.14. Contractor shall optimize pricing and terms for all Third-Party Assets.

2.4.2.15. Contractor shall provide Integrated Asset Management data for analytics for trending, forecasting, planning to facilitate decisions based on Asset information.

2.4.2.16. Contractor shall annually update and deliver the Integrated Asset Management Service Management plan, for County approval, and posted on the Service Portal.

2.4.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Integrated Asset Management Services.

Integrated Asset Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Design and implement an Integrated Asset Management System.	X	
2. Review and approve an Integrated Asset Management System.		X
3. Produce and submit recommended policies, processes and procedures to be added to the Standards and Procedures Manual.	X	
4. Review and approve changes to be added to the Standards and Procedures Manual.		X
5. Produce and submit recommended Asset Management monthly report format (e.g., End-User name, department, account code, location, low-org).	X	
6. Review and approve Asset management monthly report format.		X
7. Produce and submit recommended software license monthly report format.	X	
8. Review and approve recommended software license monthly report format.		X
9. Produce and submit Asset Management policies and procedures.	X	
10. Review and approve Asset Management policies and procedures.		X
11. Produce and submit software license management policies and procedures.	X	
12. Review and approve software license management policies and procedures.		X
13. Produce and submit comprehensive inventory of Assets tracked, managed and reportable through the Asset Management System.	X	
14. Review and Approve comprehensive inventory list provided by the Contractor.		X

Integrated Asset Management Roles and Responsibilities		
Build Roles and Responsibilities	**Contractor**	**County**
15. Develop operational policies standards and procedures manual for security management.	X	
16. Implement Asset Management policies and procedures.	X	
17. Implement Software License management policies and procedures.	X	
18. Implement software License monthly report.	X	
19. Implement Asset Management monthly report.	X	
20. Deploy an electronic Integrated Asset Management System that meets the County's requirements, adheres to defined policies and includes the following asset information (if applicable): • Manufacturer • Model • Serial number • Asset identification number • Asset location • Ownership information (Contractor/County - lease/purchase) • Asset cost information • Maintenance information and history including the age of the Asset and duration of contract terms • Warranty information • Other billing information (e.g., lease information, County-specific information) • Transaction edit history (e.g., locations, billing and User)	X	
21. Provide and support an electronic Integrated Asset Management System which includes asset auto discovery tools to maintain asset data and User profiles.	X	
22. Provide acquisition and tracking as required to fulfill County requests.	X	
23. Negotiate, enter into, track and manage all contracts, including licenses, with Third-Parties as required for the provision of the Services.	X	
24. Provide and support an electronic interface to the County's finance and chargeback systems to meet accounting, tracking, and reporting requirements.	X	
25. Develop and implement online access to Asset Management information.	X	

Integrated Asset Management Roles and Responsibilities		
26. Implement and support interfaces to feed asset location and financial data, including Third-Party data such as relevant taxation, book and depreciation value data to an online reporting dashboard.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Track and manage all Assets provided by the Contractor.	X	
28. Conduct periodic reviews and provide exception reports resulting from use of asset auto discovery tools.	X	
29. Produce and submit monthly reports on Assets.	X	
30. Produce and submit copies of all Third-Party contracts, including licenses, upon request of the County.	X	
31. Produce and submit monthly software license management report.	X	
32. Review and approve monthly software license management report.		X
33. Validate compliance with applicable software licensing agreements using automated software tools and manual processes as required.	X	
34. Verify installed software for non-networked PCs (that periodically touch the network to check E-Mail, for example), while those PCs are in contact with the network.	X	
35. Report any license compliance issues no more than 30 days from the date of the issue.	X	
36. Report on contract expirations, license changes/upgrades, etc. in advance to prevent disruptions in service, non-compliance issues, etc.	X	
37. Report any expiration or renewal requirements for Assets to allow for planning and mitigation.	X	
38. Manage the ordering, procurement and delivery processes in compliance with County procurement and acceptance processes.	X	
39. Maintain version control on asset inventory.	X	
40. Dispose Assets (e.g. donation, sale, disposal) per County direction and generally acceptable accounting and financial standards or requirements.	X	
41. Provide reports of Asset Management review results.	X	

Integrated Asset Management Roles and Responsibilities		
42. Provide and, upon County approval, implement Asset Management remediation plan for Asset Management deficiencies.	X	
43. Review and approve review reports and remediation plans of Asset inventory management information.		X
44. Provide reports of County asset financial information including depreciation, maintenance contracts and value of Assets.	X	
45. Conduct periodic/ad hoc quality assurance review of Integrated Asset Management System.		X

2.5. Billing Management Services

2.5.1. Overview

Billing Management Services consist of the activities and processes associated with the timely and accurate billing for the Services. Billing Management Services shall collect consumption data for all Frameworks, calculate all charges and billing information, produce and provide invoices to the County, provide chargeback details that meet the County's requirements, and provide all necessary support to ensure the timely and accurate processing of both the invoice and chargeback.

2.5.2. High Level Requirements

2.5.2.1. Contractor shall digitally interface its Contractor billing system with the County chargeback management system (iTrack).

2.5.2.2. Contractor shall manage and support the operational availability of the iTrack to Oracle Financials interface.

2.5.2.3. Contractor shall use a billing program that efficiently and effectively handles the tracking of billable resources and maintains a direct interface to the Integrated Asset Management Services.

2.5.2.4. Contractor shall make provide, for County approval, all process and procedural documentation pertaining to Billing Management Services.

2.5.2.5. Contractor shall provide accurate and timely invoices with an appropriate level of detail.

2.5.2.6. Contractor shall promptly provide accurate and timely detailed electronic billing information that facilitates the County's chargeback activities.

2.5.2.7. Contractor shall support all activities required to review, validate, substantiate, and detail its billings.

2.5.2.8. Contractor shall work with the County to optimize the invoice and chargeback process, including continuous improvement of reporting and automation.

2.5.2.9. Contractor shall communicate to County information impacting the billing of resources.

2.5.2.10. Contractor shall provide details for any billing inquiries to support the costs billed to the County or invoiced to the County upon request.

2.5.2.11. Contractor shall annually update and deliver the Billing Management Services Management plan, for County approval, and posted on the Service Portal.

2.5.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Billing Management Services.

Billing Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommended policies, processes and procedures to be added to the Standards and Procedures Manual.	X	
2. Review and approve changes to be added to the Standards and Procedures Manual.		X
3. Identify chargeback and reporting requirements.		X

Billing Management Services Roles and Responsibilities		
4. Identify monthly invoicing requirements.		X
5. Produce and submit recommended monthly invoice/billing report format in accordance with County requirements.	X	
6. Review and approve monthly billing report format.		X
7. Document and maintain invoicing requirements.	X	
8. Participate in, and support, billing reviews as requested by the County.	X	
Build Roles and Responsibilities	**Contractor**	**County**
9. Provide an automated interface with the County's finance system for Billing Management Services.	X	
10. Provide an automated interface with the County's chargeback system in accordance with County requirements, including the ability for the County to review the chargeback reports and supporting data online through the Service Portal without any delays.	X	
11. Produce and submit monthly reports (both hardcopy and electronically) detailing all usage and charges.	X	
12. Maintain an electronic repository of all Billing Management records (reports, invoices, chargeback, etc.) for the duration of the contract.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Contractor shall verify staff enter billable time on a daily basis for accurate tracking of project costs.	X	
14. Produce and submit to County chargeback reports and monthly invoices.	X	
15. On a monthly basis, meet with the County's finance staff to review invoices including: • Provide a mock invoice for review and agreement • If discrepancies are identified, clarify and resolve them • Meet again within a week to reach agreement on the changes or clarifications so the submitted invoice can be signed off	X	
16. Approve chargeback reports.		X
17. Download on a monthly basis all usage and charge information to the County chargeback application.	X	
18. Provide invoices per County requirements.	X	

Billing Management Services Roles and Responsibilities		
19. Document and maintain County chargeback reporting requirements.	X	
20. Calculate, report, and chargeback all applicable taxes and provide monthly billing for current and past services as well as track payments and balances.	X	
21. Provide the billing data needed to reconcile bills.	X	
22. Approve invoices.		X
23. Maintain and provide an electronic archive of all billing and its details.	X	
24. Retain all source system data used for billing to provide audits trails or verification of details for the duration of the Agreement.	X	

2.6. Security Management Services

2.6.1. Overview

The Security Management Services Framework Component within the Cross Functional Framework applies to the discipline of designing, implementing and maturing security practices to protect critical County business processes and Assets across the enterprise.

2.6.2. High Level Requirements

2.6.2.1. Contractor shall provide the continuous improvement in overall security services that protect the County.

2.6.2.2. Contractor shall provide a qualified Chief Information Security Officer (CISO), with County approved, that will work directly with the County CISO.

2.6.2.3. Contractor shall ensure Contractor assigned CISO is not directly involved in the management of day-to-day operations.

2.6.2.4. Contractor CISO shall work with the Contractor assigned CTA to ensure strategic alignment with architecture standards and guidelines.

2.6.2.5. Contractor shall develop strategic risk guidance for Service Requests, including the evaluation and recommendation for technical controls.

2.6.2.6. Contractor shall participate in architecture and strategy sessions with the County to determine and maintain the Security Management roadmap.

2.6.2.7. Contractor shall work with each Service Framework to ensure alignment, training, validation, compliance with Security Management Services.

2.6.2.8. Contractor shall ensure confidentiality of all Hardware and Software used to provide the Services.

2.6.2.9. Contractor shall ensure the availability of all Hardware and Software providing the Services is only used for its intended purpose.

2.6.2.10. Contractor shall design, develop, procure, implement and monitor a strategic, and continuously improving comprehensive security and risk management program to protect the integrity, confidentiality and availability of County Data and the Services.

2.6.2.11. Contractor shall establish a hierarchical security governance program that includes the formation of an information security steering committee which includes the County and Contractor staff and provides for the centralized governance of security services.

2.6.2.12. Contractor shall design, develop, implement, maintain and publish up-to-date information security policies, procedures, training, standards and guidelines to the Service Portal.

2.6.2.13. Contractor shall, with County CISO approval, create and manage information security and risk management awareness training programs for End-Users, Third-Party and approved system users.

2.6.2.14. Contractor shall design, develop, implement and maintain risk assessment and risk management processes for the Services.

2.6.2.15. Contractor shall, with the County CISO approval, design, develop and maintain categories for information ownership, classification, accountability and protection.

2.6.2.16. Contractor shall continuously assess and improve the Security Management Services against an industry-standard maturity model.

2.6.2.17. Contractor shall perform all necessary security-related reviews and annually attest to security compliance for delivering the Services.

2.6.2.18. Contractor shall use the NIST Computer Security Resource Center (CSRC) security framework as a guide for Security Management Services.

2.6.2.19. Contractor shall continuously monitor security and risk environmental factors for evolving trends and threats.

2.6.2.20. Contractor shall develop and implement plans to remediate any identified threat.

2.6.2.21. Contractor shall develop and maintain an annual Security life cycle report for the Services.

2.6.2.22. Contractor shall design, develop, implement and maintain a security incident management and response plan, for County approval, and post to the Service Portal.

2.6.2.23. Contractor shall provide periodic executive reports on the "State of Security" which includes the overall effectiveness, efficiency, maturity and other relevant matters related to the Services.

2.6.2.24. Contractor shall develop a security information and event management (SIEM) solution and the required set of operational procedures in defining, using and maturing the processes.

2.6.2.25. Contractor shall maintain Federal and State compliance to security for any applicable County program, application or other Service.

2.6.2.26. Contractor shall annually update and deliver the Security Management Services Management plan, for County approval, and posted on the Service Portal.

2.6.2.27. Contractor shall provide the Enterprise Application Access (EAA) solution.

2.6.2.27.1. EAA integrates data path protection, identity and access management (IAM), application security, multi-factor authentication (MFA), single sign-on (SSO), and management visibility and control into a unified service across all application locations and types (on-premises, Internet, IaaS, SaaS, etc.).

2.6.2.27.2. EAA will be implemented on all active applications (PA, CA, IA) to the enterprise portal.

2.6.2.27.3. EAA will be implemented on all County departments, San Diego County Sheriff Department, San Diego County District Attorney and San Diego County Employees Retirement Association and be available to associated subcontractors, partners and citizens in support of the County.

2.6.2.28. Contractor shall provide the Multi-Factor Authentication (MFA) solution.

2.6.2.28.1. The MFA Service integrates with County EAA solution to provide advanced multi-function authentication functionality across all County applications using supported EAA MFA methods (e.g., FIDO/FIDO2; SMS; Hardware OTP; Software OTP; Push).

2.6.2.28.2. The MFA Service is implemented across all County departments for users of County shared applications including County subcontractors performing work on

behalf of County, partners and Contractor staff supporting the Agreement.

2.6.2.28.3. The County EAA Service is extended to the County of San Diego Sheriff's Department, County of San Diego District Attorney's Office and to San Diego County Employees Retirement Association, to the extent required to access County applications using the County MFA solution.

2.6.2.29. Contractor shall provide the Malware Protection solution to all County websites protected by the Akamai Web Application Firewalls.

2.6.2.29.1. Malware Protection shall protect web apps and Application Programming Interface (APIs) from malicious file uploads by scanning file uploads at the Akamai edge.

2.6.2.29.2. Malware Protection shall integrate with Akamai Web Application Firewall to detect and block malware at the Akamai edge by scanning files once, at the edge, to avoid setting scanning at every application.

2.6.2.30. Contractor shall provide the Secure Internet Access (SIA) solution to all County managed devices.

2.6.2.30.1. SIA shall provide a cloud-based secure web gateway (SWG) that protects County network.

2.6.2.30.2. SIA shall proactively block requests to known malware, phishing, command and control, and Domain Name System (DNS) data exfiltration domains.

2.6.2.30.3. SIA shall block malicious payload downloads with improved zero-day protection before they compromise endpoint devices.

2.6.2.30.4. SIA shall protect devices when on and off the network, including mobile devices.

2.6.2.30.5. SIA shall protect all outbound DNS traffic including Internet of Things (IoT), servers and peripherals.

2.6.2.30.6. SIA shall provide detection/prevention of zero-day phishing attacks.

2.6.2.30.7. SIA shall enforce acceptable use policies.

2.6.2.30.8. SIA shall block categories of domains.

2.6.2.30.9. SIA shall provide visibility and control over internet-based applications, such as social media.

2.6.2.30.10. SIA shall control the types of files that can be uploaded/downloaded on the internet.

2.6.2.30.11. SIA shall provide web-based Data Loss Prevention (DLP) controls.

2.6.2.30.12. SIA shall include tools to identify the specific devices on the network making requests that violate the configured policy.

2.6.3. Environment

The environment scope of Security Management Services includes, but is not limited to, the following:

2.6.3.1. Technical

2.6.3.1.1. Approve appropriate methods for the protection of all Assets used for the Services.

2.6.3.1.2. Propose authentication methods, password policy, encryption methods, etc.

2.6.3.1.3. Propose rules for secure teleworking.

2.6.3.1.4. Define required security features of Internet services.

2.6.3.1.5. Define principles for secure development of information systems.

2.6.3.1.6. Review logs of user activities in order to recognize suspicious behavior.

2.6.3.2. Business continuity

2.6.3.2.1. Coordinate the business impact analysis process and the creation of response plans.

2.6.3.2.2. Coordinate exercising and testing.

2.6.3.2.3. Perform post-Incident review of the recovery plans.

2.6.3.3. Compliance

2.6.3.3.1. Develop the list of interested parties related to information security.

2.6.3.3.2. Develop the list of requirements from interested parties.

2.6.3.3.3. Remain in continuous contact with authorities.

2.6.3.3.4. Coordinate all efforts related to personal data protection.

2.6.3.4. Risk management

2.6.3.4.1. Develop Contractor training on performing risk assessment.

2.6.3.4.2. Coordinate the process of risk assessment.

2.6.3.4.3. Propose the selection of safeguards.

2.6.3.4.4. Propose the deadlines for safeguards implementation.

2.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Security Management Services.

Security Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define County requirements at the enterprise level for all security services (e.g., business, technology strategy, functional, availability, capacity, performance, applications, backup and continuity service).		X
2. Assist in developing Security standards, policies and procedures including leading industry practices.	X	
3. Produce and submit quarterly updates to security requirements, standards, procedures and policies including regulatory requirements for County approval.	X	
4. Review and approve security requirements, standards, procedures and policies for County.		X
5. Develop security patching standards relevant to the environment including asset management integration with Third-Party security vulnerability notifications services (e.g., NIST NVD).	X	
6. Review and approve security patching standards relevant to the environment.		X
7. Perform feasibility studies for the implementation of new security technologies that best meet County business needs and meet cost, performance and quality objectives.	X	

Security Management Roles and Responsibilities		
8. Participate in technical and business planning sessions to establish security standards, architecture and project initiatives.	X	
9. Conduct technical reviews and provide recommendations for improvements to the infrastructure, application development and operations that increase the overall effectiveness, efficiency and prudent resource and cost management of security.	X	
10. Produce and submit operational policies and procedures for Security Management.	X	
11. Review and approve operational policies and procedures for Security Management.		X
12. Recommend appropriate controls for individual departments that meet requirements (e.g., HIPAA, HHSA, etc.).	X	
13. Review and approve appropriate controls for individual departments meet requirements (e.g., HIPAA, HHSA, etc.).		X
14. Recommend Security Management testing and vulnerability analysis standards on a yearly basis.	X	
15. Review and approve Security Management testing and vulnerability analysis standards on a yearly basis.		X
16. Produce and submit policies and procedures for relevant to the Services and are necessary for protecting the Confidentiality, Integrity and Availability of Assets, information and resources.	X	
17. Review and approve policies and procedures for relevant to the Services and are necessary for protecting the Confidentiality, Integrity and Availability of Assets, information and resources.		X
18. Produce and submit annual security strategies and roadmaps for the Services.	X	
19. Review and approve annual security strategies and roadmaps for the Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
20. Develop and maintain a Security and Risk Management Manual.	X	
21. Review and approve the Security and Risk Management Manual.		X
22. Develop and maintain a Risk Assessment Process and Procedure Manual.	X	

Security Management Roles and Responsibilities		
23. Review and approve the Risk Assessment Process and Procedure Manual.		X
24. Identify relevant and applicable standards and methods to apply to County systems and applications to meet all special statutory and regulatory objectives and requirements.	X	
25. Comply with all statutory and regulatory requirements associated with the delivery of the Services, requirements regarding systems, including specific regulatory requirements for systems affiliated with the California Law Enforcement Telecommunications System (CLETS) and the FBI Criminal Justice Information Systems (CJIS).	X	
26. Evaluate and provide risk reduction and cost effectiveness of security processes and procedures.		X
27. Review all security patches relevant to the environment and classify the need and speed in which the security patches must be installed.	X	
28. Maintain all documentation required for security reviews and internal control and control testing.	X	
29. Recommend encryption technologies, security monitoring, anti-virus programs and relevant patches and upgrades as required by County policies and standards.	X	
30. Review and approve encryption technologies, security monitoring, anti-virus programs and relevant patches and upgrades as required by County policies and standards.		X
31. Design a web-based security dashboard that displays metrics, aggregated security log data across all frameworks, and enable total security awareness of the County's security environment.	X	
32. Review and approve the web-based security dashboard that displays metrics, aggregated security log data, and enable total security awareness of the County's security environment.		X
33. Develop and recommend improvement plans for Locations as needed to maintain effective physical security.	X	
34. Review and approve physical security improvement plans for Locations.		X
35. Develop and document technical design plans and environment configuration based on County security requirements.	X	

Security Management Roles and Responsibilities		
36. Review and approve all adjustments to County security policies, regulations and procedures as a result of new service features and components.		X
37. Produce and submit System and Application security procedures.	X	
38. Review and approve System and Application security procedures.		X
Operate Roles and Responsibilities	**Contractor**	**County**
39. Conduct security assessments and report monthly on vulnerabilities and recommended mitigations.	X	
40. Conduct scheduled review meetings between the Contractor's security officer and the County security officer and related security working group(s).	X	
41. Support County requested internal and Third-Party security reviews, vulnerability and penetration testing.	X	
42. Support periodic reviews of security practices, process and procedures as required by County.	X	
43. Review the County's security policies annually and work with the County security officer to recommend updates, additions, or changes as the County's working environment changes.	X	
44. Develop and maintain a Security Risk Registry of all identified County security risks.	X	
45. Create and maintain a secured online repository for all Security related documents and artifacts (e.g., Customer Service Request Forms, Security Assessments, Security Audits, Security Roadmaps, Risk Assessments, etc.).	X	
46. Review and validate management and current updates are performed to the Security on-line repository.		X

2.7. Service Delivery Management (SDM) Services

2.7.1. Overview

This section pertains to Service Delivery Management Services Cross Functional Framework Component. Each County Business Group (FG3, CSG, PSG, HHSA and LUEG) has a single, assigned Service Delivery Manager. The Service Delivery Manager(s) shall act as a liaison to the Business Group with respect to all Services, including but not

limited to, operational support, billing management, escalation management, change management, release management, Incident management, Problem management, availability and capacity management, Service Request status, communications and service continuity in the event of unplanned outages, declared emergency or disaster.

The Enterprise Service Delivery Manager shall interface directly to the CTO and shall coordinate the delivery of Services to the assigned Business Group Service Delivery Managers. The Business Group Service Delivery Manager shall continuously receive and assess customer feedback in order to improve overall service delivery goals.

2.7.2. High Level Requirements

2.7.2.1. Contractor shall recommend, for County approval, a qualified Service Delivery Manager as Contractor Key Personnel that reports to CTO.

2.7.2.2. Contractor shall recommend, for County approval, qualified Business Group Service Delivery Managers as Contractor Key Personnel to manage Service Delivery Management Services.

2.7.2.3. Contractor Service Delivery Manager shall be familiar with ITIL and have experiences in a variety of frameworks including but not limited to, Service Desk, End-User Services, Network Management, Data Center Management, Change Management, Program Management, application delivery, and Release Management.

2.7.2.4. Contractor shall define and maintain, for County approval, processes for all Service Delivery Manager Services.

2.7.2.5. Contractor Service Delivery Managers shall maintain and build relationships with County Business Groups and departments.

2.7.2.6. Contractor Service Delivery Managers shall handle all Incident and Problem escalations and trending to provide consistency to the level of service quality.

2.7.2.7. Contractor shall work collaboratively with the County to ensure the most efficient and effective use of SDM resources and processes.

2.7.2.8. Contractor shall annually update and deliver the Service Delivery Management Service Management plan, for County approval, and posted on the Service Portal.

2.7.3. Contract and Acquisition Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with SDM Services.

SDM Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop SDM job standards and requirements.	X	
2. Review and approve SDM job standards and requirements.		X
3. Provide resumes of SDMs meeting the approved standards and requirements.	X	
4. Select a SDMs meeting the approved standards and requirements.		X
5. Produce and submit SDM Services policies and procedures.	X	
6. Review and approve SDM Services policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Implement SDM Services policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Perform internal SDM activities to ensure a high-level of performance and quality across all Service Frameworks.	X	
9. Audit Contractor Operations and Maintenance activities for compliance with Operational policies & procedures.		X
10. Produce and submit results of internal reviews relating to the County's service frameworks.	X	
11. Review and approve internal review findings.		X
12. Incorporate review findings into County Service frameworks as necessary to maintain compliance.	X	

SDM Management Roles and Responsibilities		
13. Recommend resolutions to address recurring operational Problems or Incidents.	X	
14. Review and approve resolutions to address recurring operational Problems or Incidents.		X
15. Track and report recurring operational Problems or Incidents and provide associated consequences of Problems or Incidents if there is a business impact to the County.	X	
16. Ensure that recurring operational Incidents are reviewed using root cause analysis processes and implement corrective actions as appropriate.	X	
17. Routinely assess customer satisfaction at program and service element levels using automated survey tool.	X	
18. Initiate additional survey processes as required to measure Contractor's performance rating.		X
19. Report results and trend analysis of customer satisfaction surveys with corrective action plans, as needed, in the monthly status report.	X	
20. Periodically review selected functions to verify that established policies and procedures are being followed and, if variances are noted, recommend corrective actions.	X	
21. Perform periodic internal reviews to check that standards are being followed.	X	
22. Perform regular reviews of Contractors services and performance against Service Levels and other performance measures.	X	
23. Lead and manage internal delivery teams to review incidents, problems and any other operational Incidents affecting client production and non-production environments.	X	
24. Drive the Contractor teams to remediate the problems and provide root cause analysis as needed.	X	
25. Review change management requests and participate in Change Management Boards.	X	
26. Provide a consolidated monthly report on service delivery information, challenges and insights.	X	

2.8. [Reserved]

2.9. Project Management Services

2.9.1. Overview

Project Management Services defines the structured effort to manage risk that achieves expected results. Project Management Services shall deliver products, Assets, change and/or components within agreed resources and a defined start and end time.

2.9.2. High Level Requirements

2.9.2.1. Contractor shall provide qualified program and project management resources with relevant background and experience including PMI certification.

2.9.2.2. Contractor shall recommend, for County approval, qualified Project Management Office Manager as Contractor Key Personnel to manage Project Management Services.

2.9.2.3. Contractor PMO shall report directly to the Contractor Account Management team.

2.9.2.4. Contractor PMO shall establish continuous mentoring and training for Project Managers.

2.9.2.5. Contractor shall define standards, methods and best practices that shall be used in the delivery of Project Management Services.

2.9.2.6. Contractor shall establish centralized tracking and reporting for all projects accessible from the Service Portal.

2.9.2.7. Contractor shall define all processes in the delivery of Project Management Services and that are posted on the Service Portal.

2.9.2.8. Contractor shall define measurements to ensure the delivery of projects on time, on budget and in scope.

2.9.2.9. Contractor shall implement, with County approval, a standardized project management methodology that incorporates industry typical practices. This methodology shall be used by the Contractor in providing all of the Services.

2.9.2.10. Contractor shall annually update and deliver the Project Management Services Management plan, for County approval, and posted on the Service Portal.

2.9.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Project Management Services.

Project Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for standard project management tools, reports, and artifacts.	X	
2. Review and approve standard project management tools, reports, and artifacts.		X
3. Produce and submit recommendations for project-specific tools and artifacts.	X	
4. Review and approve project-specific tools and artifacts.		X
5. Produce and submit resource-loaded project plans for all projects.	X	
6. Review and approve resource-loaded project plans for all projects.		X
7. Produce and submit project status reports on no less than a monthly basis.	X	
8. Provide a range of training options in the service catalog.	X	
9. Produce and submit project management policies and procedures.	X	
10. Review and approve project management policies and procedures.		X
11. Recommend business process reengineering methodologies.	X	

Project Management Roles and Responsibilities		
12. Assess and approve business process re-engineering methodologies.		X
13. Identify opportunities for business process improvements.	X	
14. Provide industry knowledge applicable to County departmental business to identify opportunities for business process reengineering and Application development and integration/modification.	X	
Build Roles and Responsibilities	**Contractor**	**County**
15. Develop operational policies standards and procedures manual for Project Management Services.	X	
16. Implement County authorized Project Management discipline.	X	
17. Work in conjunction with the County's training and development resources to provide a common look and feel to training delivery methods.	X	
18. Implement and manage County-authorized Project Management tools and processes based on industry standards.	X	
19. Develop and maintain a training course catalog in cooperation with County HR and the Business Groups to provide End-Users access to training so they can develop the necessary skills to fulfill their responsibilities.	X	
20. Implement approved project management policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
21. Support project management policies and procedures.	X	
22. Provide high quality project management for all initiatives and projects undertaken as part of the Services.	X	
23. Participate in Program management and Project management activities as required to ensure successful work efforts.		X
24. Facilitate project status reviews with County management and staff on no less than a monthly basis.	X	
25. Track projects through timekeeping tool and biweekly status reports.	X	
26. Distribute the standard project processes, templates, or other vehicles, to all stakeholders to collect relevant project operational and performance data.	X	

Project Management Roles and Responsibilities		
27. Support the County's Verification & Validation activities including assisting in identifying errors, risk factors, omissions, discrepancies, constraints, performance and security Incidents, and other obstacles in project implementations.	X	
28. Provide local venues for training, particularly for Cross-Functional Services training or special purpose training when delivering training to Users in their environment is not practical (e.g., when providing training on new systems or applications for which a computer laboratory type environment is necessary and shall be leveraged across many training sessions).	X	
29. Provide project planning, tracking and management of project activities.	X	
30. Document project lessons learned and summarize the outcomes of the project.	X	
31. Ensure that all changes to the project are reviewed and approved in advance by coordinating all changes across the project and notifying stakeholders of approved changes.	X	
32. Approve project changes.		X
33. Examine project issues to determine their impact to the analysis or project effort.	X	
34. Categorize risks within a project and analyze as to the consequences, probability, impact, exposure, mitigation, contingency and triggers.	X	

2.10. Integration and Testing Services

2.10.1. Overview

Integration and Testing Services are the activities associated with ensuring that all individual components configured with or added to the environment work together cohesively to achieve the intended results. The following table identifies the Integration and Testing roles and responsibilities that Contractor and County shall perform.

2.10.2. High Level Requirements

2.10.2.1. Contractor shall conduct tests integration or interfaces between components, interactions to different parts of the system such as an

operating system, file system and hardware or interfaces between systems.

2.10.2.2. Contractor shall develop and deliver, for County approval, and implement a methodology and tool sets for conducting Integration and Testing Services.

2.10.2.3. Contractor shall update annually the methodology for conducting Integration and Testing Services.

2.10.2.4. Contractor shall continuously update tools sets used for conducting Integration and Testing Services.

2.10.2.5. Contractor shall verify functional, performance, and reliability requirements are placed on major design items.

2.10.2.6. Contractor shall detect any inconsistencies between the software units integrated together or between any of the instances of the standard hardware.

2.10.2.7. Contractor shall define and maintain, for County approval, processes for all Integration and Testing Services

2.10.2.8. Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.10.2.9. Contractor shall annually update and deliver the Integration and Testing Services Management plan, for County approval, and posted on the Service Portal.

2.10.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Integration and Testing.

Integration and Testing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Integration and Testing Services Roles and Responsibilities		
1. Define Integration and Testing requirements and policies.		X
2. Develop, document and maintain in the Standards and Procedures Manual Integration and Testing procedures that meet requirements and adhere to defined policies.	X	
3. Review and approve Integration and Testing procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Develop operational policies standards and procedures manual for Integration and Testing.	X	
5. Define Test requirements.		X
6. Manage and schedule integration test environment.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Maintain software release matrices across development, QA, and production environments and Networks.	X	
8. Validate and approve the software release matrix.		X
9. Evaluate all new and upgraded components or services for compliance with County security policies, regulations and procedures.	X	
10. Validate new and upgraded components or services for compliance with County security policies, regulations and procedures, as required.		X
11. Assess and communicate the overall impact and potential risk to components prior to testing completion.	X	
12. Conduct integration and security testing for all new and upgraded equipment, Networks, software or services to include unit, system, integration and regression testing based on requirements defined in requirements and design documents.	X	
13. Stage new and upgraded equipment, software or services to smoothly transition into existing environment based on requirements defined in requirements and design documents.	X	
14. Perform modifications and performance-enhancement adjustments to County system software and utilities as a result of changes to architectural standards or additions and upgrades to the environment.	X	

Integration and Testing Services Roles and Responsibilities		
15. Test new releases of supported Hardware and Software to ensure required performance and functionality is maintained in conformance with County Service Levels.	X	
16. Provide Middleware required to integrate Software and Hardware.	X	
17. Support Middleware required to integrate Software and Hardware.	X	
18. Provide integration of application software.	X	

2.11. Incident Management Services

2.11.1. Overview

Incident Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with restoring service operations to County End-Users. Incident Management will restore unplanned disruption to the Services as quickly as possible while providing minimal impact to County business operations. An Incident is any unplanned event, which causes an interruption or a reduction to the quality of the Services.

The Service Desk is responsible for primary ownership of recording and tracking all Incidents and is responsible for the close coordination and ongoing monitoring and tracking of, and reporting on, Incidents. The Service Desk shall be responsible for escalating Incidents and coordinating with all appropriate Tier 2, Tier 3 and Tier 4 support groups.

The Incident Management processes and activities are inter-related and complementary with Change Management, Release Management and Configuration Management, as well as Problem Management.

2.11.2. High Level Requirements

2.11.2.1. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Incident Management Services.

2.11.2.2. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Incident Management methodology.

2.11.2.3. Contractor shall own, record and track all Incidents end-to-end.

2.11.2.4. Contractor shall follow all defined Service Level priorities for all Incidents.

2.11.2.5. Contractor shall assume the highest severity for any Incident lacking complete clarity.

2.11.2.6. Contractor shall immediately communicate with the County CTO of all Severity 1 and Severity 2 Incidents.

2.11.2.7. Contractor shall define, document and continuously maintain an Incident Response Team for all Severity 1 and Severity 2 Incidents.

2.11.2.8. Contractor shall investigation and diagnosis all Incidents.

2.11.2.9. Contractor shall develop and deliver an RCA for all Severity 1 and Severity 2 Incidents or ad-hoc Incidents as requested by County.

2.11.2.10. Contractor shall develop and post escalation procedures for Incidents Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.11.2.11. Contractor shall annually update and deliver the Incident Management Services Management plan, for County approval, and posted on the Service Portal.

2.11.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Incident Management Services.

Incident Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Establish criteria for Incident Management support requirements, including equipment and services to be covered, severity levels, definitions and characteristics, Incident classification and prioritization schema, escalation requirements.		X

Incident Management Services Roles and Responsibilities		
2. Develop Incident Management policies, process and procedures that support County's Incident Management support requirements.	X	
3. Review and approve Incident Management policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Develop operational policies standards and procedures manual for Incident Management.	X	
5. Provide and continuously maintain an Incident Management system and knowledge management database, including all Hardware, Software, databases, automated monitoring tools, and management and reporting tools, which are acceptable to County.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
6. Provide unrestricted read access by County-authorized staff and other personnel to all current and historical Incident records and knowledgebase data.	X	
7. Monitor the Incident Management system for automatically generated and logged Incident alerts and events.	X	
8. Resolve Incidents on the first call in accordance with the Procedures Manual, knowledge database documents, and configuration database(s).	X	
9. Identify, filter, and classify Events and Incidents to a severity level and handle according to agreed-upon Incident response procedures.	X	
10. Diagnose and resolve Incidents; where possible use desktop remote control with user's approval and disconnecting when complete. Where possible, implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved Incidents).	X	
11. Escalate Incidents to the appropriate next-level service group within Contractor, County, or Third-Party service as soon as it is clear that the Incident is unable to be resolved without additional assistance or as required to comply with Service Level response times.	X	
12. Monitor and track Incident resolution progress through to final closure and record/update Incident record status as appropriate.	X	

Incident Management Services Roles and Responsibilities		
13. Provide expert functional and process assistance for applications at Tier 1 and escalate to Tier 2 or 3 resource as required.	X	
14. Provide Tier 1 assistance to inquiries on the features, functions and usage of Hardware and Software.	X	
15. Provide Tier 1 support for applications software on the supported applications.	X	
16. Propose training and Tier 1 scripts and workarounds for the Service Desk for applications software on the approved list.	X	
17. Approve training and Tier 1 scripts and workarounds for the Service Desk for applications software on the approved list.		X
18. Provide Tier 2 and Tier 3 support for Applications software on the supported applications list.	X	
19. Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed/resolved Incident.	X	
20. Assist End-Users with questions relating to functionality and use of End-User Hardware and Software.	X	
21. Document solutions to resolved Incidents in central knowledgebase. Accurately update all information pertinent to Incidents including general verbiage, codes, et al.	X	
22. Notify designated County personnel of all Severity 1 and Severity 2 Incidents within the designated timeframe.	X	
23. Contact designated County business personnel of applicable Severity 1 and Severity 2 Incidents.		X
24. Maintain current and historical records of all calls and the resolution of those calls for the life of the contract and provide reporting and trends.	X	
25. Troubleshoot, diagnose and resolve Incidents for all Hardware and Software warranty and non-warranty devices, including removing and / or repairing physically broken or inoperable devices.	X	
26. Provide Dispatch for End-User devices as required.	X	
27. Provide end-to-end Incident Identification, Escalation and Resolution Management; and a Closure Process including the management of those Incidents escalated to Third-Parties.	X	

Incident Management Services Roles and Responsibilities		
28. Track ongoing status of any Incident and their corresponding Incident record to ensure that identified Incidents are addressed and resolved.	X	
29. Ensure Incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	X	
30. Coordinate and take ownership of Incident resolution across all Frameworks with County and Third-Parties.	X	
31. Periodically review the status of open, unresolved Incidents and related Incidents and the progress being made in addressing Incidents.	X	
32. Participate in Incident Management review sessions as appropriate.	X	
33. Conduct Incident review sessions and provide listing and status of same categorized by Incident severity impact.	X	
34. Participate in Incident Management review sessions.		X
35. Coordinate with County and Third-Party Tier 2 support groups to acquire and transfer knowledge on Incident resolution and record this knowledge gained into the knowledge base to facilitate increased ability for Third-Party Tier 1 Service Desk in providing first-call resolution.	X	
36. Conduct follow-up with End-Users who reported the Incident to verify that the Incident was resolved to the End-User satisfaction.	X	
37. Close out Incidents that were resolved satisfactorily.	X	
38. Provide Incident Management reporting as required.	X	

2.12. Problem Management Services

2.12.1. Overview

Problem Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated of resolving not-yet-known root cause behind one or more Incidents.

The Problem Management processes and activities are inter-related and complementary with Change Management, Release Management and Configuration Management, as well as Incident Management.

2.12.2. High Level Requirements

2.12.2.1. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Problem Management Services.

2.12.2.2. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Problem Management Services methodology.

2.12.2.3. Contractor shall own all reported or diagnosed Problems end-to-end.

2.12.2.4. Contractor shall develop and implement proactive problem management for Incidents and identify trends to prevent future Incidents.

2.12.2.5. Contractor shall provide Problem Management Services for all identified Problems and systemic Incidents related to the Services.

2.12.2.6. Contractor shall provide coordination and assistance to Third-Party in performing for Problem Management Services.

2.12.2.7. Contractor shall provide reactive Problem Management Services by diagnosing and solving Problems in response to one or more Incidents.

2.12.2.8. Contractor shall maintain, update and report information about Problems and the appropriate workarounds and resolutions.

2.12.2.9. Contractor shall continuously work to reduce the number and impact of Incidents and Problems occurring within the County.

2.12.2.10. Contractor shall be responsible for ensuring that resolutions to Problems are implemented in a timely fashion.

2.12.2.11. Contractor shall fully document and deliver, for County review, all Problems including symptoms through final resolution.

2.12.2.12. Contractor shall prevent recurrence of Incidents related to these errors by determining the unknown underlying cause (e.g., root cause) and resolving them.

2.12.2.13. Contractor shall annually update and deliver the Problem Management Services Management plan, for County approval, and posted on the Service Portal.

2.12.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Problem Management Services.

Problem Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define requirements and policies for Problem Management (e.g., events that trigger a Root Cause Analysis (RCA), categorization and prioritization schema, etc.).		X
2. Participate in developing Problem Management requirements and policies.	X	
3. Develop appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.	X	
4. Approve appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Problem Management.	X	

Problem Management Services Roles and Responsibilities		
6. Implement appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.	X	
7. Establish and maintain a Problem Management knowledgebase (Service Portal) that is accessible to County where information about Problems, Root Cause, Known Errors, Workarounds and problem resolution actions will reside.	X	
8. Provide unrestricted access by County-authorized staff and other County designated personnel to all current and historical Problem Management records and knowledgebase data.	X	
9. Ensure Problem Management activities conform to defined Change Management procedures set forth in the Procedures Manual.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Coordinate with appropriate Incident Management teams and take ownership of Problem Management activities of all problems determined to reside in the Frameworks.	X	
11. Coordinate, escalate and track Problem Management activities within County and Third-Parties related to problems determined to reside in all infrastructure areas.	X	
12. Flag all Incidents that require further RCA to be conducted (i.e., Severity 1 and Severity 2 Incidents) per the agreed-to procedures.	X	
13. Ensure that recurring problems that meet defined criteria related to the Contractor's service responsibility area are reviewed using RCA procedures.	X	
14. Conduct proactive trend analysis of Incidents and problems, and other data elements to identify recurring situations that are or have the potential to be indicative of future problems and points of failure.	X	
15. Track and report on problems and trends or failures and identify associated consequences of problems.	X	
16. Develop and recommend corrective actions or solutions to address recurring Incidents and problems, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis.	X	

Problem Management Services Roles and Responsibilities		
17. Identify, develop, document, and recommend appropriate Workarounds for known errors of unresolved problems and notify Incident Management and all other appropriate stakeholders of its availability if approved. Document the workaround in the knowledgebase.	X	
18. Review and approve Workarounds for implementation, as appropriate.		X
19. Coordinate and monitor status of root-cause analysis activities performed by County and Third-Party.	X	
20. Document and update Problem Management knowledgebase with information regarding problem resolution actions, activities and status (e.g., root cause, known errors, workarounds, etc.) and notify all appropriate stakeholders of availability of information.	X	
21. Coordinate with County and Third-Party service to ensure that knowledge on Problems related to Frameworks is captured and entered into a centralized Problem Management knowledgebase.	X	
22. Ensure problem resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	X	
23. Provide status reports detailing the root cause and procedure for correcting recurring Problems and Severity 1 and Severity 2 Incidents until closure as determined by County.	X	
24. Conduct Problem Management review meetings and provide listing and status of same categorized by problem impact.	X	
25. Participate in Problem Management review meetings and review and approve recommendations for actions, where appropriate.		X
26. Periodically review the state of open Incidents and related problems and the progress being made in addressing Problems.	X	
27. Participate in and review and approve as appropriate all Problem Management generated Request for Change (RFCs) as part of the Change Management.		X
28. Create Request for Change (RFC) documentation with recommended corrective actions to be taken to resolve a problem and submit to County for review and approval.	X	
29. Conduct periodic problem management proactive review sessions.	X	

Problem Management Services Roles and Responsibilities		
30. Provide Problem Management reporting on a weekly basis for all activity.	X	

2.13. Change Management Services

2.13.1. Overview

Change Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with standardized methods and procedures that are used for efficient and prompt handling of all changes. Change Management Service apply to all changes across all Frameworks, and minimize the impact of any change to the quality and operation of the Services.

The Change Management processes and activities are inter-related and complementary with Release Management and Configuration Management, as well as Incident Management and Problem Management.

2.13.2. High Level Requirements

2.13.2.1. Contractor shall develop, deliver (for County approval), post to Service Portal and continuously maintain standardized methods and procedures for Change Management Services.

2.13.2.2. Contractor shall develop process for handling Hardware and Software version control through Change Management Services.

2.13.2.3. Contractor shall establish a centralized control point for Change Management Services.

2.13.2.4. Contractor shall ensure minimal conflict and potential service disruption for all changes.

2.13.2.5. Contractor shall eliminate and prevent all unauthorized changes to the Services.

2.13.2.6. Contractor shall implement maintenance windows for changes affecting the Services.

2.13.2.7. Contractor shall minimize the amount of emergency changes to the Services.

2.13.2.8. Contractor shall record all changes made to the Services.

2.13.2.9. Contractor shall ensure all changes are evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner with County participation.

2.13.2.10. Contractor shall post on the Service Portal all documentation, changes requests, approvals, or any other information related to the Change Management Services.

2.13.2.11. Contractor shall determine metrics for measuring effectiveness of a changes and will post monthly report on the Service Portal.

2.13.2.12. Contractor will coordinate and manage, with County participation, the Change Advisory Board (CAB).

2.13.2.13. Contractor shall ensure County approval is received for all changes are deemed approved.

2.13.2.14. Contractor shall establish and manage the schedule of approved changes Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.13.2.15. Contractor shall annually update and deliver the Change Management Services Management plan, for County approval, and posted on the Service Portal.

2.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Change Management Services.

Change Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Change Management Services Roles and Responsibilities		
1. Define Change Management policies and requirements, including change priority schema and classifications, per the Change Management process components outlined above.		X
2. Develop Change Management procedures, communications venues and processes per the Change Management process components outlined above.	X	
3. Participate in the development of the Change Management and CAB procedures, policies, communications venues and approval authorities.		X
4. Review and Approve Change Management process, procedures and policies.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Change Management.	X	
6. Oversee the approved change build, test, change communication and implementation processes to ensure these activities are appropriately resourced and completed according to change schedule.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Receive and document all Requests for Change (RFC) and classify proposed changes to the Services.	X	
8. Review and validate that RFCs comply with Change Management policies, procedures, and processes.		X
9. Ensure that appropriate back-out plans are documented and in place in the event of systems failure as a result of the change.	X	
10. Provide Change Management plan to County for review.	X	
11. Review and approve Change Management plan.		X
12. Recommend change management communication venues.	X	
13. Review and approve change management communication venues.		X
14. Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes or FSC) for County to review.	X	

Change Management Services Roles and Responsibilities		
15. Coordinate, schedule, and conduct Change Advisory Board (CAB) meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies.	X	
16. Provide change documentation as required, including proposed metrics as to how effectiveness of the change to be measured.	X	
17. Review and approve change documentation and change effectiveness metrics.		X
18. Review and approve any RFC determined to have significant risk impact to the Services.		X
19. Authorize and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures.		X
20. Publish and communicate the approved FSC to all appropriate IT and Business Group stakeholders within County of change timing and impact.		X
21. Participate in business risk assessment for change to be introduced without being fully tested.	X	
22. Monitor changes, perform change reviews and report results of changes, impacts, and change effectiveness metrics.	X	
23. Verify that change met objectives based upon predetermined effectiveness metrics and determine follow-up actions to resolve situations where the change failed to meet objects.	X	
24. Review and approve change management results.		X
25. Close out RFCs that met the change objectives or changes that were abandoned.	X	
26. Perform Change Management quality control reviews and reviews of Change Management processes, and records.		X
27. Provide County Change Management reports as required and defined by County.	X	

2.14. Release Management Services

2.14.1. Overview

Release Management Services Framework Component of Cross Functional Services are the roles and responsibilities that are concerned with implementing approved changes to the Services. Release Management Services are activities that take a holistic view of scheduled changes to the Services and ensure that the technical and non-technical dependencies of the release. Release Management Service encompasses the planning, design, build, configuration and testing of hardware and software releases to create a defined set of release policies and procedures.

The Release Management processes and activities are inter-related and complementary with Change Management and Configuration Management, as well as Incident Management and Problem Management.

2.14.2. High Level Requirements

2.14.2.1. Contractor shall establish standardized Release Management policies and procedures, for County approval, and post to the Service Portal.

2.14.2.2. Contractor shall manage the release plans and schedules for approved changes.

2.14.2.3. Contractor shall develop, deliver and continuously manage release documentation.

2.14.2.4. Contractor shall develop, deliver, and continuously manage the release design, build, and configuration processes.

2.14.2.5. Contractor shall implement release testing, if appropriate, for all approved changes.

2.14.2.6. Contractor shall document, deliver and post on the Service Portal rollout planning including quality plans and back-out plans for releases.

2.14.2.7. Contractor shall document, deliver and post on the Service Portal all release communication, preparation, and training.

2.14.2.8. Contractor shall manage the rollout/distribution and installation of all elements of a release.

2.14.2.9. Contractor shall document each release and shall update the Configuration Management Database (CMDB).

2.14.2.10. Contractor shall annually update and deliver the Release Management Services Management plan, for County approval, and posted on the Service Portal.

2.14.3. Environment

2.14.3.1. Releases

Releases consist of a number of corrective action fixes and enhancements to the Services. A Release consists of the new or changed software required and any new or changed Hardware needed to implement the approved changes. Categories of releases are below:

- Major Software releases and Hardware upgrades or replacements, normally containing large areas of new functionality. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes
- Minor Software releases and Hardware upgrades, normally containing small enhancements and fixes. A minor upgrade or release usually supersedes all preceding emergency fixes
- Emergency Software and Hardware fixes, normally containing the corrections to a small number of known Incidents

2.14.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Release Management Services.

Release Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Release Management policies and requirements per the Release Management process components outlined above.		X
2. Develop Release Management procedures and processes per the Release Management process components outlined above.	X	
3. Participate in the development of the Release Management process and procedures and policies.		X
4. Review and approve Release Management process procedures and policies.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Release Management.	X	
6. Establish and maintain an appropriate secure environment(s) where all authorized versions of all Software, in physical or electronic form as applicable (Definitive Software Library or DSL) and where all hardware spares (Definitive Hardware Store or DHS) are stored, protected and accounted.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Maintain master copies of all new versions of Software (both COTS Software packages and application developed custom-built Software) in the secured DSL and update configuration item.	X	
8. Ensure that all hardware spares are secured in the DHS and reflected in the configuration management database(s).	X	
9. Establish, manage, update, and maintain the overall Release Plan and Release Schedule for all planned Releases.	X	
10. Establish and administer the version control schema as it relates to Release Management of County custom applications.	X	
11. Develop, manage, update and maintain formal Release Plans for each Release in coordination with Change Management.	X	
12. Develop quality plans and back-out plans as appropriate for each Release.	X	
13. Provide Release Management Plans and Schedules to County for review.	X	
14. Review and approve Release Management Plans and Schedules.		X

Release Management Services Roles and Responsibilities		
15. Conduct site surveys, as necessary, to assess existing Hardware and Software being used to validate Release package requirements and dependencies.	X	
16. Plan resource levels and requirements for supporting a release.	X	
17. Ensure that any new Software, Hardware, or support services required for the release are procured and available when needed.	X	
18. Ensure that all necessary testing environments are available and properly configured to support Release testing.	X	
19. Ensure there is segregation of duties between the application developer testers and the release management testers.	X	
20. Conduct post-deployment testing as required.	X	
21. Schedule and conduct Release Management meetings to include review of planned releases and results of changes made.	X	
22. Identify and document all Configurable Items (CIs) that need to be included in the Release, as well as all system inter-dependencies.	X	
23. Plan and manage the acceptance testing process for each Release.	X	
24. Review and approve Release acceptance testing plans.		X
25. Provide Release documentation as required.	X	
26. Authorize and approve scheduled Releases or alter the schedule as defined in the Release Management procedures.		X
27. Review Release Management details and alter as appropriate to meet the needs of the County (e.g., back out plan, go/no go decision).	X	
28. Notify County of Release timing and impact and provide communications to the Service Desk.	X	
29. Implement Release in compliance with Change Management requirements and adherence to detailed release plans.	X	
30. Modify configuration database, Asset Management items, and service catalog (if applicable) to reflect changes to CIs due to the Release.	X	

Release Management Services Roles and Responsibilities		
31. Conduct post-mortem of Releases that necessitated implementation of the back out plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.	X	
32. Perform quality control reviews and approve Release control results.		X
33. Provide County Release Management reports as required and defined by County.	X	

2.15. Configuration Management Services

2.15.1. Overview

Configuration Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with the recording, tracking, updating and disseminating the County's configurations for all Assets. Configuration Management Services will provide an integrated Configuration Management Database (CMDB), will capture all logical configurations of Hardware and Software supporting the Services, contain mappings to physical configuration, inventory data of Hardware and Software, analyze trends and be used to manage and reduce Incidents and Problems.

The Configuration Management processes and activities are inter-related and complementary with Change Management and Release Management, as well as Incident Management and Problem Management.

2.15.2. High Level Requirements

2.15.2.1. Contractor shall deliver and maintain an integrated Configuration Management Database (CMDB).

2.15.2.2. Contractor shall make available the CMDB through the Service Portal for approved County End-Users.

2.15.2.3. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Configuration Management Services.

2.15.2.4. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Configuration Management methodology.

2.15.2.5. Contractor shall own Configuration Management end-to-end.

2.15.2.6. Contractor shall monitor, optimize, maintain, document, and report on all County Hardware and Software configurations, including but not limited to new releases and versions, patches, and bug fixes.

2.15.2.7. Contractor shall update the CMDB promptly after the completion of any approved change or release.

2.15.2.8. Contractor shall identify configuration items, control and manage changes to configuration items, provide status accounting of those changes, verify functional and physical characteristics of configuration items, release and deliver configuration items.

2.15.2.9. Contractor shall perform configuration identification, control, status accounting, reviews and release management according to County policies and procedures.

2.15.2.10. Contractor shall use a tool set or suite of tools to ensure application configuration and code management is securely stored, managed and accessible as the system of record for configuration management and code management.

2.15.2.11. Contractor shall provide an enterprise code version manager to be the central repository for Portfolio Application configurations, patch downloads, software downloads, custom code, scripts and any software asset required to maintain or restore Portfolio Applications.

2.15.2.12. Contractor shall support, maintain and manage the enterprise code version manager including updates to ensure functionality and currency for code release, code deployment and accessibility.

2.15.2.13. Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.15.2.14. Contractor shall annually update and deliver the Configuration Management Services Management plan, for County approval, and posted on the Service Portal.

2.15.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Configuration Management Services.

Configuration Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit configuration management policies, procedures and policies.	X	
2. Review and approve configuration management policies, procedures and standards.		X
3. Produce and submit recommendations for configuration changes.	X	
4. Review and approve configuration changes.		X
5. Establish and maintain a single approach to manage both the County Configuration Management Database (referred to as the Unified Configuration Management Database) and the Integrated Asset Management System in accordance with the County's requirements.	X	
6. Monitor Third-Party announcements regarding software upgrades, patches, reported Incidents and published solutions.	X	
7. Provide impact analysis and propose installation plans for announced fixes.	X	
8. Recommend the applications packages that can be regularly reviewed for patches or version release upgrades and review this list per a defined schedule.	X	

Configuration Management Services Roles and Responsibilities		
9. Identify and report when patches or version-release upgrades are available for Applications and determine which functionalities are newly available as a result of the upgrade or which system Incidents are addressed by it, particularly when this improves customer ease of use.	X	
10. Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes.	X	
11. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing.	X	
12. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items.		X
13. Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.	X	
14. Develop procedures for establishing security baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.		X
15. Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies.	X	
Build Roles and Responsibilities	**Contractor**	**County**
16. Implement and maintain configuration management policies and procedures.	X	
17. Establish a Change and Release Control Board (CRCB) that approve CM policies and their inclusion in Standards and Procedures in the County Standards and Procedures Manual, and shall approve or delegate approval of changes and releases of updates.	X	
18. Provide the County Standards and Procedures Manual for CRCB for County Approval.	X	
19. Approve the County Standards and Procedures Manual for CRCB.		X
20. Participate in Change and Release Control Board (CRCB) and review and approve CRCB activities and decisions.		X

Configuration Management Services Roles and Responsibilities		
21. Select, install and maintain configuration management tools.	X	
22. Ensure and follow change control and notification processes for installations, upgrades and adjustments to components, software and County processes.	X	
23. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing.	X	
24. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and regressing of configuration items.	X	
25. Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states.	X	
26. Establish process for verifying the accuracy of configuration items; adherence to configuration standards, management process and the identification of process deficiencies.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Perform configuration management.	X	
28. Identify when configuration item changes or updates affect other services.	X	
29. Install manufacturer field change orders, service packs, firmware, and software maintenance releases, etc.	X	
30. Perform configuration management activities throughout the system life-cycle.	X	
31. Perform configuration management activities throughout the development life cycle.	X	
32. Perform configuration management and change management activities related to integration and testing.	X	
33. Perform product patch, “bug fix,” service pack installation or upgrades to the current installed version.	X	
34. Review configuration management results and accuracy of configuration data.		X
35. Correct any inaccurate configuration data and CIs.	X	

Configuration Management Services Roles and Responsibilities		
36. Maintain master copies of new versions in a secured software library and update configuration databases.	X	
37. Administer the version control system as it relates to release management of County Applications.	X	
38. Ensure that inventory and configuration management records are maintained and that all updates to County and Contractor records are reflected.	X	
39. Provide document version control for all documentation for which Contractor is responsible.	X	
40. Inform the County of changes through the weekly change and release control meetings and periodic integrated change status reporting. Each change request shall identify other related change requests to facilitate integrated reporting.	X	

2.16. Capacity Planning and Performance Management Services

2.16.1. Overview

Capacity Planning and Performance Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with optimizing the efficiency, effectiveness, capacity and technical performance of the Hardware and Software performing the Services. Capacity Planning and Performance Management Services will provide process of determining the resources required, will prevent performance or availability impact to County business, develop and manage services response time and quality of services for End-Users.

The Capacity Planning and Performance Management processes and activities are inter-related and complementary with Change Management and Release Management, as well as Incident Management and Problem Management.

2.16.2. High Level Requirements

2.16.2.1. Contractor shall monitor and manage systems to leverage and optimize the Services.

2.16.2.2. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and

processes related to Capacity Planning and Performance Management Services.

2.16.2.3. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Capacity Planning and Performance Management methodology.

2.16.2.4. Contractor shall own Capacity Planning and Performance Management end-to-end and across all Service Frameworks.

2.16.2.5. Contractor shall analyze historical resource usage by tracking and trending Hardware and Software performing the Services.

2.16.2.6. Contractor shall continuously perform capacity analysis across the Hardware and Software performing the Services.

2.16.2.7. Contractor shall develop, deliver (for County approval) and implement a capacity plan on an annual basis for Hardware and Software performing the Services.

2.16.2.8. Contractor shall develop, deliver (for County approval), and implement a on a monthly basis a list of tuning activities for Hardware and Software performing the Services.

2.16.2.9. Contractor shall continuously monitor, measure, forecast and post to the Service Portal capacity actuals, historical resource use trends and corrective actions on a monthly basis.

2.16.2.10. Contractor shall model short-term and long-term resource usage and performance based on proposed approved releases.

2.16.2.11. Contractor shall identify and implement improvements to better leverage existing capacity.

2.16.2.12. Contractor shall communicate potential capacity or performance Incidents to the County in advance, and implement approved solutions in a timely manner.

2.16.2.13. Contractor shall annually update and deliver the Capacity and Performance Management Services Management plan, for County approval, and posted on the Service Portal.

2.16.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Capacity Planning and Performance Management Services.

Capacity Planning and Performance Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Conduct capacity planning activities that incorporate all Systems, sub-systems, and software, workload balancing, and resource allocation.	X	
2. Develop or provide tools to monitor capacity and performance.	X	
3. Review and approve tools to monitor capacity and performance.		X
4. Recommend changes to capacity to improve service performance.	X	
5. Approve capacity-related recommendations.		X
6. Produce and submit recommendations for changes to optimize capacity management.	X	
7. Review and approve changes to optimize capacity management.	X	
8. Produce and submit projections prior to the start of each contract year regarding estimated usage and loading for all Service Frameworks based on historical trends, anticipated new projects and decommissioning of systems, etc.	X	
9. Develop and maintain a capacity plan to meet the County's existing and future needs. The process components of the capacity Management plan shall include: • Application sizing • Resource forecasting • Demand forecasting • Modeling • Performance monitoring • Workload monitoring	X	
10. Perform Application capacity and performance planning by incorporating business projections provided by the County.	X	

Capacity Planning and Performance Management Services Roles and Responsibilities		
11. Perform capacity and performance planning on an ongoing basis when new business and application growth is anticipated, when changes to existing business requirements are anticipated or occur, or when system configuration changes are performed.	X	
Build Roles and Responsibilities	**Contractor**	**County**
12. Implement comprehensive capacity management planning process as well as tools to monitor capacity and performance.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Maintain capacity levels to optimize use of existing resources and minimize County costs to deliver Services in accordance with the Service Levels.	X	
14. Monitor and manage capacity in all Service Frameworks to maximize performance and efficiency and to minimize service disruptions.	X	
15. Assess impact/risk and cost of capacity changes and submit mitigation recommendations.	X	
16. Continually monitor resource usage to enable proactive identification of capacity and performance Incidents.	X	
17. Capture trending information and forecast future County capacity requirements based on County defined thresholds.	X	
18. Assess capacity impacts when adding, removing or modifying Applications.	X	
19. Assess Incidents/Problems related to throughput performance.	X	
20. Recommend and perform approved DBMS tuning changes.	X	
21. Conduct periodic database reorganizations as indicated by usage and performance.	X	
22. Define and execute database performance and tuning scripts and keep database running at optimal performance for County's workload.	X	
23. Implement and administer appropriate database management tools across all database instances.	X	
24. Validate asset utilization and capacity efficiency.	X	
25. Participate in all capacity planning activities.		X

Capacity Planning and Performance Management Services Roles and Responsibilities		
26. Perform Framework Component tuning to maintain optimum performance in accordance with Change Management procedures.	X	

2.17. Disaster Recovery Management Services

2.17.1. Overview

The Disaster Recovery (DR) Framework Component within the Cross Functional Framework applies to the process for resumption of County business after a disruptive event. Disaster Recovery Management Services will provide strategy, process, type, methodology, locations, documentation and prompt restoration of the Services.

Disaster Recovery Management Services planned and implemented as part of the Data Center Framework. Types of DR to consider would be:

- Active/Active – synchronous
- Active/Passive – asynchronous
- Active/Passive – vault

Contractor shall propose a plan, during transition, to execute for Disaster Recovery Services. The plan should consider the following:

- Portfolio Applications priorities and RTO/RPO requirements
- Active/Active-synchronous methodology
- Active/Passive – asynchronous methodology
- Active/Passive – vault methodology
- Data Synchronization and replication plans
- Reduce licensing costs
- Validation that restoration times meet the requirement of the Service Levels

2.17.2. High Level Requirements

2.17.2.1. Contractor shall develop the type of DR that will be used to support the Services.

2.17.2.2. Contractor shall execute the DR plan upon County declaration of a disruptive event.

2.17.2.3. Contractor shall recover and resume full operations of Severity 1 applications, including all supporting infrastructure and network within 48 hours.

2.17.2.4. Contractor shall recover and resume full operations of Severity 2 applications, including all supporting infrastructure and network within 72 hours.

2.17.2.5. Contractor shall recover all County Data repositories with a data loss of no greater than 28 hours.

2.17.2.6. Contractor shall provide, for County approval, the initial and executable DR plan during the Transition period.

2.17.2.7. Contractor shall submit, for County approval, annual updates to the DR plan.

2.17.2.8. Contractor shall review the County's Business Continuity Plans and use in the development of the DR plan.

2.17.2.9. Contractor shall ensure the DR plan covers all the Service Frameworks.

2.17.2.10. Contactor shall adjust the DR plan with new items that the County, in writing, deems necessary.

2.17.2.11. Contractor shall implement the full DR plan prior to the conclusion of Transition.

2.17.2.12. Contractor shall implement changes, if any, within three (3) months related to the County approved annual DR plan.

2.17.2.13. Contractor shall update the DR plan based on technology related environmental changes and updates.

2.17.2.14. Contractor shall create, update and maintain working procedures for execution of the DR plan in the Standards and Procedures Manual.

2.17.2.15. Contractor shall perform an annual test of the DR plan.

2.17.2.16. Contractor shall provide a full report, for County approval, of the DR plan annual test.

2.17.2.17. Contractor shall correct any discrepancies discovered in the annual DR test within three (3) months Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.17.2.18. Contractor shall annually update and deliver the Disaster Recovery Management Services Management plan, for County approval, and posted on the Service Portal.

2.17.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with DR Management Services.

DR Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a DR plans that meets County requirements.	X	
2. Review and approve the DR plan that meets County requirements.		X
3. Produce and submit data recovery plan consistent with the County's business requirements.	X	
4. Review and approve data recovery plan.		X
5. Produce and submit at the start of each Contract Year a revised DR Plan to continually meet County objectives.	X	
6. Review and approve the yearly DR Plan.		X
7. Produce and submit a yearly DR test plan.	X	
8. Approve the DR test.		X
9. On an annual basis, review the prioritization of application portfolio and reclassify, if required, priority levels.	X	
10. Designate the criticality recovery level for each application in the County application portfolio.	X	

DR Management Services Roles and Responsibilities		
11. Review and approve the assigned criticality levels.		X
Build Roles and Responsibilities	**Contractor**	**County**
12. Design and implement DR plan.	X	
13. Design and implement data recovery plan.	X	
14. Coordinate the DR plans with the County Technology Office plans to address any potential disconnects or misunderstanding.	X	
15. Submit yearly DR test Plans to the County.	X	
16. Perform yearly DR test.	X	
17. Submit yearly DR test results to the County.	X	
18. Review and approve yearly DR test results.		X
19. Maintain and document requirements for off-site data storage.	X	
20. Review documentation for off-site data storage.		X
Operate Roles and Responsibilities	**Contractor**	**County**
21. Provide secure offsite storage for designated media and transport media to offsite location as required (include handling, storing, shipping, and receiving media).	X	
22. Ensure archived data is available for use in disaster recovery operations.	X	
23. Provide off-site backup media storage.	X	
24. Establish and maintain contracts for hot-site or cold-site availability as required, coordinate disaster recovery exercises to ensure readiness, and perform required recovery.	X	
25. Promote DR by meeting with the County's CIO, governance committees, the business managers, and the departments to provide appropriate communication during any DR operation.	X	
26. Perform scheduled DR tests per County policies, requirements and the DR Plan.	X	
27. Track and report DR test results to the County.	X	
28. Approve DR testing results.		X
29. Perform corrective action identified during the DR test and provide ongoing status until completion.	X	

DR Management Services Roles and Responsibilities		
30. Provide a written DR test and corrective action report to the County by a mutually agreed upon date each year.	X	
31. Execute DR Procedures when directed by an authorized representative of the County.	X	
32. Provide DR recovery within Service Levels from the time a disaster is declared for Priority 1 Applications.	X	
33. Provide DR recovery within the Service Levels from the time a disaster is declared for Priority 2 Applications.	X	
34. Provide DR recovery within the specified Service Levels from the time a disaster is declared for all required Applications to support Priority 1 and 2 Applications.	X	

2.18. Identity Access Management Services

2.18.1. Overview

Identity Access Management (IAM) Services Framework Component of the Cross Functional Framework applies to the business processes that facilitates the management of electronic identities. The IAM Framework Component includes all the technology, services and support needed to support identity management.

2.18.2. High Level Requirements

2.18.2.1. Contractor shall submit, for County approval, and implement an executable IAM plan to consolidate County identities into a single, federated IAM solution.

2.18.2.2. Contractor shall federate and maintain identities into the IAM solution per County Service Request.

2.18.2.3. Contractor shall provide, for County approval, the initial and executable IAM plan during the Transition period.

2.18.2.4. Contractor shall participate in architecture and strategy sessions with the County to determine and maintain the IAM roadmap.

2.18.2.5. Contractor shall develop automated workflow to manage access Service Requests.

2.18.2.6. Contractor shall implement automation tool for IAM to initiate, capture, record and manage End-User identities and their related access permission.

2.18.2.7. Contractor shall follow County policy in the provision of IAM Services

2.18.2.8. Contractor shall ensure that the IAM solution is reviewable and in compliance with any applicable regulatory process.

2.18.2.9. Contractor shall ensure the maintenance of overall security for the IAM solution.

2.18.2.10. Contractor shall track, maintain and review End-Users access privileges who migrate to different jobs within the County.

2.18.2.11. Contractor shall implement IAM with a centralized directory service that is scalable.

2.18.2.12. Contractor shall implement IAM to facilitate the process of user provisioning and account setup with a controlled and automated workflow.

2.18.2.13. Contractor shall provide monthly reporting on all changes to the IAM repository.

2.18.2.14. Contractor shall retain all Service Requests for IAM Services that can be used for review and reporting.

2.18.2.15. Contractor shall provide automated interface to County PeopleSoft application for employee IAM Services.

2.18.2.16. Contractor shall identify and manage non-County users distinctly from County employees.

2.18.2.17. Contractor shall provide attestation functionality to be used for identity management.

2.18.2.18. Contractor shall implement and maintain synchronization of all non-IAM End-User accounts across disparate applications or cloud-based services.

2.18.2.19. Contractor will continuously consolidate disparate End-User accounts into IAM.

2.18.2.20. Contractor shall implement IAM as the single solution for all County identity services.

2.18.2.21. Contractor shall provide the capability for Portfolio Applications to integrate and use the enterprise single sign-on.

2.18.2.22. Contractor shall maintain the Service Desk for all End-User IAM related Service Requests.

2.18.2.23. Contractor shall annually update and deliver the Identity Access Management Services Management plan, for County approval, and posted on the Service Portal.

2.18.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Identity Access Management Services.

Identity Access Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommended processes for Identity Access Management authentication and authorization.	X	
2. Review and approve processes for Identity Access Management authentication and authorization.		X
3. Produce and submit escalation procedures for quick termination.	X	
4. Review and approve escalation procedures for quick termination.		X

Identity Access Management Services Roles and Responsibilities		
5. Produce and submit End-User Identity Access Management architecture.	X	
6. Establish and manage process to support temporary access.	X	
7. Review and approve End-User Identity Access Management architecture.		X
8. Produce and submit annual End-User account consolidation plan.	X	
9. Review and approve annual End-User account consolidation plan.		X
10. Produce and submit the format for a report detailing all County End-User accounts and End-User data permissions.	X	
11. Review and approve the format for a report detailing all County End-User accounts and End-User data permissions.		X
12. Develop a service ordering process that clearly defines how to order change or delete services.	X	
13. Define logging and archiving policies and requirements.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Implement systems to centrally manage and maintain Account Management data and activities.	X	
15. Implement approved processes for Identity, Access and Account Management authentication and authorization.	X	
16. Implement reports detailing all County End-User accounts and End-User data permissions.	X	
17. Implement End-User account consolidation plan.	X	
18. Analyze account management architecture and the access control systems of the County's business applications, and develop and implement an End-User Account Consolidation Plan and End-User Identity, Access and Account Management architecture that provides a platform for account synchronization across the enterprise and across disparate systems.	X	
19. Implement End-User Account Management architecture.	X	
20. Implement escalation procedures for quick termination.	X	
21. Provide logging and archiving specifications/design.	X	

Identity Access Management Services Roles and Responsibilities		
22. Approve logging and archiving specification/design.		X
Operate Roles and Responsibilities	**Contractor**	**County**
23. Centrally maintain End-User accounts.	X	
24. Perform End-User account maintenance to include account creation, deletion or modification.	X	
25. Perform End-User account password resets.	X	
26. Perform End-User authorized data permission requests.	X	
27. Facilitate the receipt and tracking of requests for End-User account activation, changes and terminations.	X	
28. Facilitate the creation, change and deletion of End-User accounts.	X	
29. Coordinate as necessary with other specialized areas to manage End-User accounts.	X	
30. Maintain Access Control Lists (ACL) in accordance with policies.	X	
31. Provide report detailing all County End-User accounts and End-User data permissions on a monthly basis.	X	
32. Provide, update and maintain a reviewable record of security modifications and produce reports and notifications of End-User access modifications, transfers, and terminations.	X	
33. Provide support, including break-fix, for all Identity, Access and Account Management Services.	X	
34. On an annual basis, update the End-User Account Consolidation Plan to reflect progress toward reduction of User IDs and credentials, and to make recommendations for implementation of new technologies within the Identity, Access and Account Management architecture.	X	
35. Support and maintain Identity, Access and Account Management technology solution for infrastructure.	X	
36. Perform engineering, configuration and ongoing management of Identity, Access and Account Management technology solution.	X	
37. Log and archive User/account activity according to approved logging and archiving specification/design.	X	

Identity Access Management Services Roles and Responsibilities		
38. Periodically review production system access logs and activities to identify malicious or abnormal behavior in accordance with established County policies and standards.	X	
39. Periodically review all County account IDs to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.		X
40. Periodically review all privileged User accounts to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.	X	
41. Periodically review End-User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	
42. Periodically review privileged User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	

2.19. Reporting Management Services

2.19.1. Overview

Reporting Management Services Framework Component of the Cross Functional Framework applies to the activities associated with the development, generation and submission of deliverables defined in Schedule 5 of the Agreement.

In addition, Contractor shall report system management information (e.g., performance metrics, and System accounting information) to the County in an on-line dashboard and electronic reports.

2.19.2. High Level Requirements

2.19.2.1. Contractor shall provide accurate and timely reporting on performance, trends, Incidents, Assets, and other topics as required by the County.

2.19.2.2. Contractor shall provide, for County approval, the initial and executable Reporting Management Services Management Plan during the Transition period.

2.19.2.3. Contractor shall ensure Reporting Management Services is fully implement prior to the end of Transition.

2.19.2.4. Contractor shall update and maintain the Reporting Management Services Management Plan on an annual basis.

2.19.2.5. Contractor shall post the County approved, Reporting Management Services Management Plan to the Service Portal.

2.19.2.6. Contractor shall post all Schedule 5 deliverables to the Service Portal.

2.19.2.7. Contractor shall develop, with County approval, all deliverables are comprehensive and detailed.

2.19.2.8. Contractor shall maintain and provide electronic online dashboards on the Service Portal for Performance Metrics.

2.19.2.9. Contractor shall annually update and deliver the Reporting Management Services Management plan, for County approval, and posted on the Service Portal.

2.19.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Reporting Management Services.

Reporting Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define reporting requirements, format and frequency.		X
2. Assist the County to identify recurring reporting and format requirements to support the County's needs for information.	X	
3. Produce and submit Reporting operational policies and procedures based on County requirements.	X	

Reporting Management Services Roles and Responsibilities		
4. Review and approve Reporting operational policies and procedures based on County requirements.		X
5. Produce and submit recommendations for measurement and reporting of Service Levels.	X	
6. Review and approve recommendations for measurement and reporting of Service Levels.		X
7. Produce and submit required County reports.	X	
8. Review and approve required County reports.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Design and implement required County reports.	X	
10. Design and implement approved recommendations for measurement and reporting of Service Levels.	X	
11. Review and approve Service Level monitoring and Reporting procedures.		X
12. Implement Reporting operational policies and procedures.	X	
13. Design an automated notification system that periodically reminds the report owner of upcoming submission dates.	X	
14. Review and approve an automated notification system that periodically reminds the report owner of upcoming submission dates.		X
15. Implement the approved automated notification system that periodically reminds the report owner of upcoming submission dates. A summary of reports due within 30, 60, and 90 days must be provided.	X	
16. Design and implement a secure Service Portal that provides the County access to web-based, self-service, customer displays of key IT metrics in a dashboard view.	X	
17. Review and approve design for a secure Service Portal that provides the County access to web-based, self-service, personalized customer displays of key IT metrics in a dashboard view.		X
18. Design and implement an automated data collection and reporting system that supports the County of San Diego's yearly budgeting process, and give the County insight into the cost details of yearly operations.	X	

Reporting Management Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
19. Produce and submit all reports and other written deliverables specified in Schedule 5 or Schedule 4.3.	X	
20. Review and approve all reports and other written deliverables specified in Schedule 5 or Schedule 4.3.		X
21. Provide the County access and input to Incident and Problem tracking system to allow for Incident/Problem monitoring and ad hoc reporting.	X	
22. Provide management reports to County on the progress of the all refresh plans.	X	
23. Report on service performance improvement results.	X	
24. Provide County configuration management reports.	X	
25. Measure and Report monthly on each Service Levels.	X	
26. Report on Service Levels performance and improvement results.	X	
27. Coordinate Service Levels monitoring and reporting with designated County representative and Third-Parties.	X	
28. Measure, analyze and provide management reports on performance relative to Service Levels.	X	
29. Conduct Service Levels improvement meetings to review Service Levels and recommendation for improvements.	X	
30. Review and approve Service Levels improvement plans.		X
31. Implement Service Levels improvement plans.	X	
32. Review and approve Service Levels metrics and performance reports.		X
33. Provide the County access to performance and Service Levels reporting and monitoring system and data.	X	
34. Produce and submit monthly reporting on Applications, showing costs broken down by Plan, Build and Operate. The Operate costs needs to be broken down into the categories unscheduled maintenance, scheduled maintenance, administration, User support, and development and integration.	X	
35. Produce and submit trend information on defects, Service Requests and estimate accuracy.	X	

2.20. Domain Name Management Services

2.20.1. Overview

Domain Name Management Services Framework Component of Cross Functional Services includes the activities required to manage all County domain names in a centralized manner. The scope includes registering new domain names, maintaining the renewal schedule, reporting of all domain names, monitoring registered domain names, and insuring overall privacy of all domain names.

Domain names are unique names that identifies and organize County web services for End-Users or external users. Domain names registered with an accredited registrar provide internet based, common name translation to the actual IP address and access to the County service.

2.20.2. High Level Requirements

2.20.2.1. Contractor shall manage all domain names on behalf of the County.

2.20.2.2. Contractor shall use an accredited registrar for all domain name registrations.

2.20.2.3. Contractor shall assume ownership of all Domain Names.

2.20.2.4. Contractor shall register all domain names as requested by a Service Request.

2.20.2.5. Contractor shall comply with the County Standards and Procedures Manual for the procedure of registering, renewing and reporting of domain names.

2.20.2.6. Contractor shall not allow a domain name to expire without prior County approval.

2.20.2.7. Contractor shall notify the County POC at least 30 days in advance of the expiration date of any Domain Name.

2.20.2.8. Contractor shall annually update and deliver the Domain Name Management Services Management plan, for County approval, and posted on the Service Portal.

2.20.3. Environment

2.20.3.1. Portfolio of Domain Names

The Contractor shall maintain the Domain Names portfolio and include the following information in the Integrated Asset Management:

- Domain name ID
- Domain name
- Type / Extension
- Renewal Date
- High Org
- Low Org
- County POC Name, E-Mail and Phone
- Secondary County POC Name, E-Mail and Phone
- Registered Name Servers
- Responding Name Servers

2.20.3.2. Reports

Contractor will provide and post on the Service Portal a monthly report containing the following information:

- Total quantity of managed domain names
- Quantity of new domain names added in the last month
- Quantity of domain names transferred 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
    - Domain name
    - Type / Extension
    - Renewal Date
    - High Org

- Low Org
- County POC Name, E-Mail and Phone
- Secondary County POC Name, E-Mail and Phone

2.20.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Domain Name Management Services.

Domain Names Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures and methodologies for managing Domain Name Management Services.	X	
2. Review and approve procedures and methodologies for managing Domain Name Management Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Implement procedures and methodologies for managing Domain Name Management Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide support, including break-fix, for all Domain Name Management Services.	X	
5. Manage and support Domain Name Management Services to meet operational and computing procedures.	X	
6. Provide and deliver monthly reports on Domain Name Management Services portfolio.	X	
7. Provide and deliver monthly notifications on renewals and expirations.	X	
8. Provide inventory reports and ensure the Integrated Asset Management sysytem contains the information for Domain Names managed by Contractor.	X	

2.21. Business Analyst Services

2.21.1. Overview

Business Analyst Services Framework Component of Cross Functional Services are the roles and responsibilities of helping County business implement technology solutions in a cost-effective manner. Business Analyst Services will provide development of business

cases, planning and monitoring, developing requirements, translating and simplifying requirements, management and communications of requirements and requirements analysis of behalf of the County business.

2.21.2. High Level Requirements

2.21.2.1. Contractor shall develop, deliver (for County approval), implement and post to the Service Portal the business analysis methodology.

2.21.2.2. Contractor shall deploy business analysts that will assist the County in transformation initiatives.

2.21.2.3. Contractor shall help County business implement technology solutions by determining requirements and communicating them effectively.

2.21.2.4. Contractor shall develop requirements management processes, tracking and reporting and documentation.

2.21.2.5. Contractor shall create Business Analyst Center that will develop relationships between Business Analysts, CTO and County business.

2.21.2.6. Contractor Business Analyst shall develop business requirements document in support of the County business engagement.

2.21.2.7. Contractor Business Analyst shall develop functional requirements in support of the County business engagement

2.21.2.8. Contractor shall annually update and deliver the Business Analyst Services Management plan, for County approval, and posted on the Service Portal.

2.21.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Business Analyst Services.

Business Analyst Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures and methodologies for Business Analyst engagement with County.	X	
2. Review and approve procedures and methodologies for Business Analyst engagement with County.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Implement procedures and methodologies for Business Analyst engagement with County.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. [blank]		

2.22. Chief Technical Architect (CTA)

2.22.1. Overview

The Chief Technical Architect (CTA) Services Framework Component of Cross Functional Services describes the roles and responsibilities that support County business by providing fundamental technology and process structure and insights for IT and Telecommunications strategies and technology standardization and by providing visibility into infrastructure, applications, and data for County business. The CTA is designated as Key Personnel under the Agreement and will be staffed accordingly.

CTA shall provide architectural and technical leadership, oversight on all projects and develop a set of cognitive roadmaps to guide the progress of the County technology year over year.

The CTA provides the bridge between the deeply technical domain architects, business analysts and solution architects and other subject matter experts to ensure that the technology infrastructure meets enterprise goals, such as adaptability and complexity reduction.

The CTA, together with the Contractor EAA and Contractor CISO, will work directly with the CTO in the development and execution of architectural direction and strategy, develop and plan enterprise initiatives, identify and track emerging trends, identify and track internal Contractor Service catalog and changes to improve overall delivered Services, anticipate and understand transformative shifts in technology, develop and maintain

enterprise and departmental roadmaps, ability to access leveraged resource subject matter experts, maintain strong relationships with leading technology partners.

The CTA shall co-chair the CIO established Enterprise Architecture governance group with responsibilities to review all requirements documentation and designs, recommending, establishing and maintaining IT standards (e.g., Bricks), patterns, IT guiding principles, and communicating decisions to all Contractor IT staff. The CTA shall post all IT standards (bricks), patterns, and guiding principles on the Service Portal as changes occur and are approved by the Enterprise Architecture governance group. At the CIO's discretion, the core group of Enterprise Architecture governance, may consist of designated CTO staff, Contractor CTA, Contractor EAA and Contractor CISO and others as the CIO may designate.

The CTA shall have overall experience in technology architecture with an understanding of application and information architecture disciplines.

2.22.2. High Level Requirements

2.22.2.1. County shall retain authority on all matters related to overall IT Architecture.

2.22.2.2. Contractor shall recommend, for County approval, qualified CTA as Contractor Key Personnel.

2.22.2.3. Contractor CTA will work directly with CTO.

2.22.2.4. Contractor CTA will develop strategy and technical direction, approved by the County, and shall have oversight on all IT projects and Contractor support staff.

2.22.2.5. Contractor shall provide a full-time, dedicated Chief Technical Architect who shall support the County's architectural planning processes and ensure high standards of technical architecture and integration in new technology-based solutions implemented for the County.

2.22.2.6. Contractor CTA shall be responsible for executing the developed strategy including adherence to methodologies, standard processes, best practices, guiding principles, and standards.

2.22.2.7. Contractor CTA shall develop architecture planning that ties all aspects of the existing technical environment to a County business-consistent desired state.

2.22.2.8. Contractor CTA shall actively participate in all IT projects to ensure that they improve the capability and maturity of the Services.

2.22.2.9. Contractor CTA shall work directly with the EAA, the CISO and CTO to develop enterprise-wide standards and initiatives.

2.22.2.10. Contactor CTA shall develop, deliver, for County approval, all technology standards, guiding principles, patterns and design guidelines and criteria. The CTA shall continuously maintain them and post them on the Service Portal.

2.22.2.11. Contractor CTA shall co-chair, with CTO co-chair, the weekly Enterprise Architecture Governance meetings. This includes setting and tracking the agenda, documenting attendance, tracking minutes and decisions, uploading all documentation to the Service Portal, and other functions to ensure the success of the meeting.

2.22.2.12. Contractor CTA shall develop and deliver, for County approval, procedures and process for weekly Enterprise Architecture Governance meetings.

2.22.2.13. Contractor CTA shall work closely with Business Analyst Services to capture new or updated County business requirements as they are developed.

2.23. Enterprise Application Architect (EAA)

2.23.1. Overview

The Enterprise Application Architect (EAA) Services Framework Component of Cross Functional Services describes the roles and responsibilities that support County business by providing governance, review and approval of requirements, solutions, designs, technology, and architecture to integrate and optimize Portfolio Applications, interfaces and integrations across the enterprise. The EAA is designated as Key Personnel under the Agreement and will be staffed accordingly.

The EAA responsibilities include, but are not limited to: reviewing 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 provides 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.

The EAA shall have overall experience in business and application architecture disciplines with an emphasis on information architecture with an understanding of technical architecture.

2.23.1. High Level Requirements

2.23.1.1. Contractor shall recommend, for County approval, qualified Enterprise Application Architect (EAA) as Contractor Key Personnel.

2.23.1.2. Contractor EAA shall work directly with CTO.

2.23.1.3. Contractor EAA shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements.

2.23.1.4. Contractor EAA shall act as a subject matter expert on the effective use of technology in developing County business solutions.

2.23.1.5. Contractor EAA shall advise IT staff regarding the feasibility of proposed approaches to project solutions in terms of systems capabilities and established application architecture guidelines and standards.

2.23.1.6. Contractor EAA shall review all requirement documents and solution designs and recommend for approval to CTO prior to any development project actions.

2.23.1.7. Contractor EAA shall review all data and information architecture to ensure that data and interfaces are optimized for application use.

2.23.1.8. Contractor EAA shall work directly with the CTA, the CISO and County CTO to develop enterprise-wide standards and initiatives.

2.23.1.9. Contractor EAA, at CIO direction, shall be a member of the Enterprise Architecture Governance Group and will participate in all scheduled meetings.

2.23.1.10. Contractor EAA shall research and track emerging technologies and concepts for solving business problems not addressed in existing, deployed technology.

2.23.1.11. Contractor EAA shall recommend standards, guiding principles and best practices for deploying business and technology solutions.

2.23.1.12. Contractor EAA shall identify gaps between current and desired end-states and recommend solutions that close and provide greater efficiencies.

2.24. Innovation Management Services

2.24.1. Overview

The Innovation Management Services Framework Component of Cross Functional Services describes the roles and responsibilities that support the continuous innovation of County business. Innovation Management Services shall have a designated Innovation Officer as Key Personnel under the Agreement and will be staffed accordingly.

Innovation Management Services shall establish a culture and environment of progressive change throughout the term of the Agreement. The Contractor shall adopt a model of continuous innovation or transformation that allows progressive change in how the Services are delivered. This includes, 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 consist of a series of initiatives in which the Contractor will develop solutions, business case analyses, proposed pricing, possible changes to the Agreement, and project timelines and resources. The proposed initiatives will be reviewed by the Innovation Management Review Board and, if approved, shall be executed using agile and rapid-prototyping methodologies.

Innovation Management Services shall include an Innovation Management Office that will serve as the foundation for continuous business improvement, innovation, and transformation. The Innovation Office shall be the hub of a set of processes, governance, and resources to sustain innovation activities, and create a true environment of agility and high-velocity change at the County, supported by the Operational and steady-state teams.

2.24.2. High Level Requirements

2.24.2.1. Contractor shall recommend, for County approval, qualified Innovation Officer (IO), as Contractor Key Personnel.

2.24.2.2. Contractor IO shall work directly with the CTO and interface directly with County business leaders.

2.24.2.3. Contractor IO will provide recommendations to staff Innovation Management Services, with County approval, starting in Year 2 of this Agreement.

2.24.2.4. Contractor AE and CIO will chair the Innovation Management Review Board (TRB) and shall have joint approval on all proposed innovation initiatives and activities.

2.24.2.5. Contractor IO and CTO shall work with the CIO and County business to get a clear understanding of the strategy, business model and direction of the County.

2.24.2.6. Contractor IO shall develop, for County approval, charter, rules of engagement, success criteria and governance process for Innovation Management Services that shall include, but not limited to, lab environment (Dev/Ops), pilot process for rapid prototyping, joint development workshops, flexible and agile process (e.g., moving to micro services or containers), renovating existing systems (e.g., Hyperconverged infrastructure).

2.24.2.7. Contractor IO shall work with the EA function to understand the business outcomes and business capabilities the County is seeking to create.

2.24.2.8. Contractor IO shall build a collaborative cross-functional Innovation Management Services core team to help drive IT innovation and transformation; create the organizational and governance model needed to drive business innovation.

2.24.2.9. Contractor IO shall track technology innovations and trends, and identify what the opportunities are for the County.

2.24.2.10. Contractor IO shall work with the internal Contractor and County IT teams, key vendors and consultants to shape a roadmap for technology innovation.

2.24.2.11. Contractor IO shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements.

2.24.2.12. Contractor shall develop the process and governance to enable the continuation of progressive change within the County.

2.24.2.13. Contractor shall continuously look for opportunities to propose innovative and transformational initiatives.

2.24.2.14. Contractor shall perform an annual assessment of Innovation Management Services, for County review and approval.

2.24.2.15. Contractor shall identify potential impacts to the Agreement and propose recommended changes based on innovation initiatives.

3. SERVICE DESK SERVICES

3.1. Overview

This section pertains to the Service Desk Services Framework. Service Desk Services consist of Plan, Build, Operate centralized services to triage, process, track, report, and resolve End-User Incidents, Service Requests and requests for information.

The Service Desk is the single point of contact (SPOC) between End-Users and the Contractor on a day-to-day basis. The Service Desk will be the focal point for reporting, logging Incidents and Service Requests for End-Users and for providing self-help information. The Service Desk shall have a high degree of interactions with End-Users, in various forms, and shall ensure that End-Users receive all services in a timely manner, 24/7/365.

The Service Desk shall provide and maintain a Service Portal that provides communications and information to all End-Users. The Service Portal will assist End-Users in entering Service Requests, reviewing current or resolved Incidents, provide user tips and FAQs on the Services and self-service functions (i.e. password resets).

The Service Desk shall support and maintain the Service Request Management Service. The Service Request Management Service shall be the system used by End-Users for installing new services, modifying current services, moving services or removing services and acts as the primary request function tool across all Frameworks.

3.2. High Level Requirements

3.2.1. Contractor shall recommend, for County approval, qualified Service Desk Manager as Contractor Key Personnel to manage Service Desk Services.

3.2.2. Contractor shall continuously improve customer service interactions and ratings.

3.2.3. Contractor shall continuously improve Incident response time and Incidents resolution.

3.2.4. Contractor shall log, track, and resolve all Incidents and Service Requests submitted from End-Users.

3.2.5. Contractor shall continuously improve County efficiency and effectiveness by providing and utilizing knowledge databases and best practices in the areas of reporting, logging, tracking, routing, resolving and reporting of Incidents and Service Requests.

3.2.6. Contractor shall develop and deliver, for County approval, chat functionality for End-Users engaging the Service Desk.

3.2.7. Contractor shall perform a closed feedback loop process, so that the handling of Incidents that are to be incorporated into lessons learned, best practices, and appropriate solutions to improve economies, efficiencies, and performance.

3.2.8. Contractor shall ensure proficient and highly skilled Service Desk support with appropriate knowledge of the Services.

3.2.9. Contractor shall provide and post all communication of modifications to the Services on the Service Portal.

3.2.10. Contractor shall provide and post all Service Levels and Service Desk statistics in a real-time, up-to-date dashboard posted on the Service Portal.

3.2.11. Contractor shall maintain a repository for all Service Desk scripts and maintain a cycle for updates and accuracy.

3.2.12. Contractor shall create and maintain a Service Portal that allows County End-Users the following:

- Access the Service Portal from the internet and the County intranet
- Create and submit Incidents and Services Requests
- View a list of all Incidents and Services Requests
- Allow End-Users to change and reset passwords
- View an up-to-date knowledge base with solutions, tip sheets and Frequently asked Questions (FAQs)
- View Countywide announcements related to the Services
- Access all Contractor deliverables

3.3. Environment

The following further describe and scope Service Desk Services elements supported by Contractor and with which Contractor shall comply.

3.3.1. Technology Refresh

Contractor shall ensure Service Desk Services maintain technical currency and refresh of all Hardware and Software used to support the Services unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

3.4. Roles and Responsibilities

3.4.1. General Roles and Responsibilities

The following table identifies the Plan, Build and Operate Service Desk Plan roles and responsibilities that Contractor and County shall perform.

Service Desk Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Service Desk solutions that best meet County business needs and service–level requirements.	X	
2. Review and approve Service Desk solutions and Service Levels.		X
3. Perform operational planning for Service Desk capacity and performance purposes.	X	
4. Perform analysis of County environment to identify the appropriate sets of skills, training, and experience needed by Service Desk staff.	X	
5. Produce and submit operational policies and procedures including escalation.	X	
6. Review and approve operational policies and procedures.		X
7. Develop Self-Help requirements and policies with input from County.	X	
8. Review and approve Self-Help requirements and policies.		X
9. Develop, document and maintain in the Standards and Procedures Manual Self-Help Support Contractor procedures that meet County requirements and adhere to County policies.	X	

Service Desk Roles and Responsibilities		
10. Review and approve Self-Help procedures.		X
11. Develop and improve Service Desk scripts as appropriate to improve performance.	X	
12. Provide all testing services required to support Service Desk Services.	X	
13. Produce and submit all test documentation to County.	X	
14. Provide all deployment services required to support Service Desk Services.	X	
15. Produce and submit to County all deployment documentation.	X	
16. Review and approve all deployment documentation.		X
Operate Roles and Responsibilities	**Contractor**	**County**
17. Provide appropriately trained Service Desk staff.	X	
18. Identify and report all recurring Incidents.	X	
19. Implement and coordinate the RCA process on Incidents and Problems in conjunction with Incident and Problem Management process.	X	
20. Perform RCA of Incidents; document findings and take corrective actions for the Services. Resolve Problems and/or substantiate that all actions taken to prevent future reoccurrence.	X	
21. Manage all Services Requests from inception to closure (e.g., recording, troubleshooting, escalating, coordinating, resolving, reporting, closing).	X	
22. Manage Incidents end-to-end.	X	
23. Provide Service Desk Services, including provision, operation and maintenance of integrated Service Desk Systems (e.g., ACD, electronic workflow, Incident Management, self-help and self-heal, knowledge database, remote desktop control, procurement management, automated provisioning) necessary to document, track and manage Incidents and Service Requests, inquiries and Incident notifications from inception to closure across Service Frameworks using cross functional processes.	X	
24. Maintain and provide Service Desk operational policies and procedures in the Service Desk knowledge database.	X	
25. Review and approve Service Desk operational policies and procedures.		X

Service Desk Roles and Responsibilities		
26. Manage and track Incidents and Service Requests that involve multiple Service Frameworks and Third-Parties and collaborate with Third-Parties to resolution and closure.	X	
27. Provide Third-Party access to the Service Desk as required to support Incidents and Service Requests (e.g. change management, Integrated Asset Management System functions).	X	
28. Utilize Service Desk to resolve Incidents and perform Service Requests (e.g., change management, Integrated Asset Management System functions).	X	
29. Provide support for inquiries on the features, functions and usage of all Portfolio Applications and OIC items in use at County.	X	
30. Perform administration services such as creating, changing and deleting End-User desktop profiles.	X	
31. Provide Self-Help services for End-Users that includes the following, at a minimum: • Password reset tool • Service Request entry, tracking, reporting, updating and status checking	X	
32. Posting of content for current Incidents, frequently asked questions, knowledgebase, and other similar elements to the Service Portal.	X	
33. Monitor and review the effectiveness and usage to End-User self-service on the Service Portal.		X
34. Develop and provide recommendations for improvements to End-User self-service on the Service Portal.	X	
35. Review and approve recommendations for improvements to End-User self-service on the Service Portal.		X
36. Implement approved recommendations for improvements to End-User self-service on the Service Portal.	X	
37. Produce and submit proposed changes to Service Desk processes, operations and procedures.	X	
38. Review and approve proposed changes to Service Desk processes, operations and procedures.		X

Service Desk Roles and Responsibilities		
39. Conduct quality assurance reviews of Service Desk documentation for accuracy and currency annually or as requested by the County.	X	
40. Develop a priority-driven Service Request handoff process consistent with defined tiers of support.	X	
41. Review and approve priority-driven Service Request handoff process for the defined tiers of support.		X
42. Recommend Service Request and Incident Management procedures.	X	
43. Identify and describe priorities, response and resolution targets for Incidents and Service Requests that have differing impacts.		X
44. Develop, document and maintain Request and Incident Management procedures in the Service Desk operational policies and procedures.	X	
45. Review and approve Service Request and Incident Management procedures.		X
46. Select and implement Software and Hardware (e.g., IVR, ACD) needed to collect, track and manage Service Requests and Incidents received by the Service Desk.	X	
47. Verify that all requests are resolved, per the End-User, prior to closure.	X	
48. Develop and maintain a list of supported Portfolio Applications including priority level and key contacts.	X	
49. Review and approve the list of supported Portfolio Applications to handle calls and routing of Incident.		X

3.4.2. Single Point-of-Contact (SPOC) Roles and Responsibilities

Single Point of Contact (SPOC) services provide toll-free support for logging, tracking, resolution and reporting of Incidents and Service Requests for the Services.

The following table identifies any Plan, Build and Operate SPOC roles and responsibilities that Contractor and County shall perform.

Single Point-of-Contact Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Single Point-of-Contact Roles and Responsibilities		
1. Recommend SPOC procedures.	X	
2. Review and approve the SPOC procedures.		X
3. Develop, document and maintain the Service Desk knowledge database with all scripts and information needed to provide Service Desk Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide access to the Service Desk knowledge database from the Service Portal to End-Users.	X	
5. Provide SPOC call-in access via a toll-free number for the Services.	X	
6. Provide SPOC and coordination for all Incidents and requests for information and Service Requests.	X	
7. Provide multiple alternative communications channels (from the Service Portal), including voice messages, E-Mail, Internet, and chat.	X	
8. Initiate Incident management process for Severity 1-3 Incidents.	X	

3.4.3. Remote Device and Software Management Roles and Responsibilities

Remote Device and Software Management Services are the activities associated with managing, maintaining and troubleshooting Hardware and Software remotely and securely over the network to minimize the need to dispatch technical personnel on-site.

The following table identifies any Plan, Build, and Operate Remote Devices and Software Management roles and responsibilities that the Contractor and County shall perform.

Remote Device and Software Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures for the Service Desk use of Remote Device and Software Management control tools.		X
2. Develop, document and maintain in the Service Desk operational policies and procedures Service Desk Remote Device and Software Management procedures that meet requirements and adhere to defined policies.	X	
3. Review and approve Remote Device and Software Management procedures.		X

Remote Device and Software Management Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
4. Each use of Remote Device and Software Management tools shall have End-User authorization.	X	
5. Diagnose Incidents using remote control tools and, when possible, implement remote corrective actions to resolve Incidents. If Resolution is not possible, escalate per the escalation procedures.	X	
6. Utilize remote controls to manage and update software, maintain configuration and inventory information, and enforce compliance standards.	X	

3.4.4. End-User Administration Services Roles and Responsibilities

End-User Administration Services are the activities associated with managing and coordinating account activation, termination, changes and expiration, and the management for End-Users.

The following table identifies any Plan, Build and Operate End-User Administration roles and responsibilities that Contractor and County shall perform.

End User Administration Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
1. Facilitate employee End-User account administration, activation, changes and terminations, including: password/account setup and reset, remote access connectivity, E-Mail accounts, End-User IDs, password resets, remote paging devices, voicemail administration, telephone lines, secure ID cards, OIC requests, etc.	X	
2. Prioritize calls to and from High Response End-Users identified in the Standards and Procedures Manual.	X	
3. Provide and maintain County escalation contact list(s).		X
4. Provide and maintain Contractor escalation contact list.	X	
5. Provide and maintain Service Desk staff access to the County Directory.	X	
6. Issue communications to Service Portal and provide status updates as required for planned and unplanned events.	X	

End User Administration Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
7. Record and maintain an up-to-date System status message that can be selected when calling the Service Desk for assistance.	X	
8. Provide End-User online status access for all requests via the Service Portal.	X	
9. Work with the Contractor operational and technical staff, as well as County, to identify solutions that minimize the need to call the Service Desk (e.g., additional End-User training, self-help opportunities).	X	
10. Approve solutions that minimize the need to call the Service Desk.		X
11. Dispatch on-site technicians as necessary.	X	
12. Categorize, prioritize and log all Incidents, Service Requests and inquiries.	X	
13. Monitor Incidents and escalate per policies and procedures until resolution.	X	
14. Diagnose and troubleshoot Incidents at the Service Desk and prior to escalation.	X	

3.4.5. IMAR (Install, Move, Add, Remove) Services Roles and Responsibilities

IMAR Services are the activities associated the end-to-end management and coordination of IMAR Service Requests including gathering the business requirements, providing authorization, logging the request, and facilitating fulfillment. All authorized IMAR requests passed automatically to the Service Desk. Examples of IMARs include, without limitation, adding Desktop Computing devices or moving network printers or a telephone handset.

The following table identifies any Plan, Build and Operate IMAR roles and responsibilities that Contractor and County shall perform.

IMAR Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit IMAR procedures for all Frameworks.	X	

IMAR Services Roles and Responsibilities		
2. Develop, document and maintain in the Service Desk operational policies and procedures the IMAR procedures.	X	
3. Review and approve IMAR procedures for all Frameworks.		X
Operate Roles and Responsibilities	**Contractor**	**County**
4. Receive and track IMAR Service Requests.	X	
5. Utilize workflow to coordinate and help perform End-User notifications and scheduling related to IMAR Service Requests.	X	
6. Confirm the requirements and scope and acquire County approval of the IMAR Service Request.	X	
7. IMAR Service Requests shall be scheduled to meet the requirements of the Service Levels.	X	
8. Approve IMAR schedule.		X
9. Coordinate approved IMAR Service Requests with Service Desk.	X	
10. Track and report status of IMAR Service Requests.	X	
11. Contact End-User to confirm completion of the IMAR Service Request.	X	
12. Verify completion of the IMAR Service Request.		X

3.4.6. Tracking and Reporting Roles and Responsibilities

The following table identifies the any Plan, Build and Operate IMAR requirements, roles and responsibilities that the Contractor and County shall perform.

Tracking and Reporting Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Annually, or as requested, recommend a list of Service Desk management reports (including standard industry KPIs).	X	
2. Review and approve updates to Service Desk management reports.		X
Operate Roles and Responsibilities	**Contractor**	**County**
3. Analyze and report on Incident trends and patterns on a monthly basis.	X	

Tracking and Reporting Roles and Responsibilities		
4. Monitor and report on Service Desk statistics and trends (e.g., Service Request volumes and trends by types of End-Users) for inclusion in the Service Portal Dashboard and Service Level reporting.	X	
5. Continuously review Incident data to detect trends, help manage high-severity Incidents and monitor training needs.	X	
6. Review report results and Service Desk operations on a monthly basis.		X
7. Provide online/access to Service Desk reports via the Service Portal.	X	
8. Track/manage/report Service Desk utilization.	X	
9. Report, monthly or sooner, repetitive Incidents, abnormal patterns of calls, and resolution recommendations.	X	
10. Review and approve recommended resolutions to the repetitive Incidents and abnormal patterns of calls.		X
11. Conduct Service Desk End-User customer satisfaction surveys on a random sample of Incidents (including both open Incidents and Incidents closed from the previous month) via an E-Mail/web-based tool.	X	
12. Provide results monthly of Service Desk End-User customer satisfaction surveys in the Service Portal.	X	
13. Produce and report on all aging Incidents and Service Requests on a monthly basis.	X	
14. Process and produce immediately tracking numbers for all reported Incidents.	X	
15. Provide reports by Enterprise, Group, Department, or Division level in the Contractor-maintained dashboard for Service Desk provided reports, statistics, and views.	X	

3.5. Service Request Management Services

3.5.1. Overview

This section pertains to the Service Request Management Services Framework Component in the Service Desk Services Framework. Service Request Management Services includes all of the services required to: enter, process, status, report Service Requests from the

County; coordinate Contractor activities to provide the Service Request; and coordinate with Third-Parties to provide the Service Request.

The Service Request Management Services is the single point tool used by End-Users to request services from the Contractor.

3.5.2. High Level Requirements

3.5.2.1. Contractor shall provide efficient and effective electronic processing of County Service Requests.

3.5.2.2. Contractor shall work with the County to develop and implement workflow policies and procedures that provide appropriate efficiency, security, and control of Service Requests.

3.5.2.3. Contractor shall coordinate its own, Subcontractor, and Third-Party resources to Service Requests.

3.5.2.4. Contractor shall provide the Service Request Management tool used to deliver the Service Request Management Services.

3.5.2.5. Contractor shall provide prompt updates to the Service Request Management tool to ensure accuracy of information presented to County End-Users.

3.5.2.6. Contractor shall provide prompt logging and routing of all Service Requests.

3.5.2.7. Contractor shall ensure that all Service Requests are accurately reported.

3.5.2.8. Contractor shall report on a monthly basis all open Service Requests.

3.5.2.9. Contractor shall process Service Requests in accordance to priorities set Standards and Procedures Manual.

3.5.2.10. Contractor shall provide solutions that meet the requirements specified by the Service Request.

3.5.2.11. Contractor shall use Service Requests to manage the workflow of all maintenance tasks and projects including the following:

- Create Service Requests to perform preventive and corrective maintenance
- Purchase parts and materials and committing inventory to a Service Requests
- Tracking the progress of a Service Requests by status
- Tracking all Service Requests costs
- Completing and closing each Service Request

3.5.2.12. Contractor shall provide access to County End-Users on the status (both current and historical) of Service Requests.

3.5.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Service Request Management Services.

Service Request Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Service Request operational policies and procedures.	X	
2. Review and approve recommendations for Service Request operational policies and procedures.		X
3. Produce and submit the Service Request Management Services design.	X	
4. Review and approve the Service Request Management Services design.		X
5. Produce and submit closed loop methodology for workflow entry, tracking and closing for Service Requests.	X	
6. Review and approve closed loop methodology for workflow entry, tracking and closing for Service Requests.		X

Service Request Management Roles and Responsibilities		
7. Produce and submit recommended monthly report format for Service Request.	X	
8. Review and approve monthly report format for Service Request.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Implement a closed loop processing for workflow entry, tracking and closing of the Service Requests.	X	
10. Implement the Service Request Management Services design	X	
11. Implement approved Service Request operational policies and procedures.	X	
12. Implement monthly Service Request reporting.	X	
13. Implement and maintain a service ordering process that clearly defines how to order, change or delete services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Ensure that all Service Requests are routed to the appropriate parties for timely resolution.	X	
15. Provide status, upon request of the County, of all Service Requests.	X	
16. Ensure applicable Service Requests are properly authorized and prioritized.	X	
17. Authorize closure of all Service Requests.		X
18. Manage efficient workflow of Service Request including the involvement of Third-Parties.	X	
19. Process all Service Requests.	X	
20. Update, as needed, the Service Request Management Services design for operational and technical currency.	X	
21. Produce and submit monthly reports detailing all Service Requests.	X	
22. Manage Service Request assignments throughout Service Frameworks and associated workflows as part of Service Desk responsibility.	X	
23. Make changes to the Service Request Management Services to account for all changes in the Services (e.g. new resource units, updated OIC) within 5 business days.	X	

4. END-USER SERVICES

4.1. Overview

This section pertains to the End-User Services Framework. End-User Services are composed of the following Framework Components:

- Desktop Computing Services
- Core Software Services
- County Retained Assets Services
- Mobile Device Support Services
- Unified Communications Services
- Catalog Services
- Network Printer Services
- Electronic File Synchronization and Sharing

4.2. High Level Requirements

4.2.1. Contractor shall recommend, for County approval, qualified End-User Service Manager as Contractor Key Personnel to manage End-User Services.

4.2.2. Contractor shall meet County business needs for highly available, reliable and secure End-User Services.

4.2.3. Contractor shall provide centralized management and control of all End-User Services.

4.2.4. Contractor shall improve End-User productivity and customer satisfaction in providing End-User Services.

4.2.5. Contractor shall continuously improve End-User Services and Service Levels.

4.2.6. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to operational and technical improvements of End-User Services.

4.2.7. Contractor shall develop training documentation and End-User FAQs and post them on the Service Portal.

4.2.8. Contractor shall continuously develop, use, maintain and update help desk scripts and processes for End-User Services support.

4.2.9. Contractor shall provide technology assistance and support to the County in planning and standard-setting activities.

4.2.10. Contractor shall standardize Hardware and Software across End-User Services.

4.2.11. Contractor shall improve asset tracking and reporting and shall provide updates to the Integrated Asset Management System.

4.2.12. Contractor shall support County's business initiatives by ensuring high performance with End-User Services.

4.2.13. Contractor shall provide Incident determination, Root Cause Analysis and Resolution for all End-User Services.

4.2.14. Contractor shall provide IMAR Services for the End-User Services.

4.2.15. Contractor shall maintain updated and publish End-User Services standards in the Standards and Procedures manual posted on the Service Portal.

4.3. Environment

The following further describe and scopes End-User Services elements supported by Contractor and with which Contractor shall comply.

4.3.1. Technology Refresh

Contractor shall refresh End-User Services as specified within each Framework Component, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

4.4. Roles and Responsibilities

4.4.1. Install, Move, Add, Remove (IMAR) Services Roles and Responsibilities

IMAR Services consist of Service Requests made by End-Users for initial deployment and provisioning of Hardware, Software, office moves, etc. The Contractor shall provide IMAR activities for the End-User Services Framework. All IMAR activities require prompt updates to the Contractor's Integrated Asset Management tracking system and monitored by the Service Desk.

The following table identifies the IMAR Services roles and responsibilities that the Contractor and County shall perform.

IMAR Services Roles and Responsibilities		
General Roles and Responsibilities	**Contractor**	**County**
1. Develop and document in the Standards and Procedures Manual IMAR procedures.	X	
2. Review and approve IMAR procedures.		X
3. Conduct pre-installation and site survey activities (e.g., Network connectivity, power, data jack preparation) in accordance with the IMAR procedures and specific Service Request.	X	
4. Perform Hardware and Software IMARs and re-installations in accordance with the Service Request, IMAR procedures and other application policies (e.g., security policies).	X	
5. Conduct data and application migration that is necessary due to any Hardware or Software IMARs and re-installations.	X	
6. Update all Cross Functional management tools (e.g., Integrated Asset Management database) with required data and Close an IMAR Service Request.	X	
7. Provide basic End-User or technical staff orientation as needed when installing a new End-User Asset.	X	
8. Coordinate with Service Desk and all other necessary Third-Party and County support organizations to manage all IMAR Service Requests to resolution and closure.	X	
9. Coordinate the disposal of obsolete Assets at the direction of the County.	X	

IMAR Services Roles and Responsibilities		
10. Conduct End-User satisfaction survey after the completion of each IMAR Service Request and End-User Assets refresh.	X	
Install Roles and Responsibilities	**Contractor**	**County**
11. Order and deliver the End-User Services Asset to the End-User workspace.	X	
12. Install the End-User Services asset, including configuration, setup, and network connection.	X	
13. Perform all diagnostic testing to ensure End-User Services Framework asset functionality.	X	
14. Remove any boxes and/or packing materials.	X	
15. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
16. Provide basic End-User or technical staff orientation when installing a new End-User Asset.	X	
Move Roles and Responsibilities	**Contractor**	**County**
17. Provide move services within a Location or from a Location to a Location, for any End-User Services Asset, which includes disconnecting, moving and reconnecting asset in accordance with the Service Request.	X	
18. Perform all diagnostic testing to ensure End-User Services asset functionality.	X	
19. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
Add Roles and Responsibilities	**Contractor**	**County**
20. Provide upgrade or add Hardware or Software to deployed End-User Services Assets in accordance with the Service Request.	X	
21. Modify current configurations to deployed End-User Services Assets to meet approved standards.	X	
22. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
Remove Roles and Responsibilities	**Contractor**	**County**
23. Provide Remove Services for End-User Services Assets that are being displaced due to Service Request, refresh or Incident.	X	

IMAR Services Roles and Responsibilities		
24. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	

4.4.2. On-Site Technical Support Roles and Responsibilities

On-Site Technical Support consists of activities conducted on-site with End-Users to resolve Incidents, execute IMARs or other Service Requests.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with On-Site Technical Support Services.

On-Site Technical Support Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit On-Site Technical Support requirements and procedures.	X	
2. Develop and document in the Standards and Procedures Manual On-Site Technical Support procedures.	X	
3. Review and approve On-Site Technical Support requirements and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Establish and maintain appropriate equipment sparing requirements and spares inventory levels for On-Site Technical Support.	X	
5. Coordinate with the Service Desk and all other necessary Contractor, Third-Party and the County support organizations to manage all On-Site Technical Support requests to Resolution and Closure.	X	
6. Coordinate with End-User or other site staff to schedule On-Site Technical Support visit in response to an Incident or Service Request.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Dispatch appropriate Tier 2 or Tier 3 technician(s) in response to an escalated Incident or Service Request.	X	
8. Troubleshoot, diagnose and resolve Incidents for all devices, including removing and/or repairing physically broken or inoperable devices or servers.	X	

On-Site Technical Support Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
9. Conduct appropriate tests of all repaired device or server to ensure the device or server is operating appropriately.	X	
10. Obtain End-User acknowledgment for completion of Service Request.	X	

4.4.3. End-User Services Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with End-User Services.

End-User Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit Hardware and Software standards for End-User Services Assets.	X	
2. Review and approve Hardware and Software standards for End-User Services Assets.		X
3. Identify, recommend and submit End-User Services solutions that best meet County's business needs.	X	
4. Review and approve End-User Services solutions.		X
5. Perform and deliver operational planning for End-User Services capacity and performance purposes.	X	
6. Recommend and submit Hardware and Software deployment/management policies and procedures.	X	
7. Review and approve Hardware and Software deployment/management policies and procedures.		X
8. Recommend and submit Hardware and Software upgrades to End-User Services Assets.	X	
9. Review and approve Hardware and Software upgrades to End-User Services Assets.		X
10. Recommend and submit updates and patches plan to End-User Services Assets.	X	
11. Review and approve updates and patches plan to End-User Services Assets.		X
12. Update and provide to Contractor a list of high response End-Users.		X

End-User Services Roles and Responsibilities		
13. Produce and submit preventive maintenance plans consistent with OEM practices. Plans shall include equipment model and manufacturer, frequency of PM, and specific actions to be taken such as cleaning, lubricating, adjusting, inspecting, running diagnostic tests, and replacing all parts and components defined by OEM as non-User replaceable or consumable necessary to keep the equipment functioning within the OEM specifications.	X	
14. Review and approve preventive maintenance plans.		X
15. Produce and submit recommendations for "right sizing" printer to employee ratios.	X	
16. Produce and submit annual printer refresh strategy to determine the actual print need compared to the installed base.	X	
17. Produce a technology roadmap two times per contract year, for all Hardware and Software components in End-User Services Framework for current and future version including end of life for support and timelines accordingly for County review.	X	
18. Review and approve submission of Contractor provided technology roadmap for all Desktop Framework Services Hardware and Software.		X
19. Continuously update the Standards and Procedures Manual with all changes to End-User Services.	X	
Build Roles and Responsibilities	**Contractor**	**County**
20. Produce and submit all design and engineering documentation required to build, deploy and support End-User Services Assets.	X	
21. Review and approve all engineering documentation required to deploy and support End-User Services Assets.		X
22. Ensure End-User Services solutions are fully integrated with the Service Desk Services and Integrated Asset Management System processes, including, but not limited to: • A shared system and database • Direct electronic interfaces between the Service Desk agents and field service technicians • Integrated support processes involving desktop, data center, and network for remote server and telephone break-fix	X	
23. Provide all test services required to support End-User Services including providing a test laboratory that develops and verifies desktop images, as well as the support of desktop Hardware and components evaluations and demonstrations.	X	

End-User Services Roles and Responsibilities		
24. Perform desktop Software (e.g., applications, patch packages) and Hardware functionality and product compatibility testing and development in the test laboratory environment using tools and procedures that are specially designed for this purpose (test to include: unit testing, system integration testing, LAN connectivity testing, load testing, and application interconnectivity testing).	X	
25. Develop and document test scripts.	X	
26. Provide documented test results/findings of all data packets and corresponding application, entering and leaving a standard desktop build for approval prior to finalizing a desktop standard image.	X	
27. Regularly monitor Third-Party websites and other communications for new application functionality, updates, and new Software or Hardware.	X	
28. Build/Acquire updates and patches for End-User Services Assets.	X	
29. Test updates and patches for End-User Services Assets.	X	
30. Produce and submit deployment plan for updates and patches for desktop assets.	X	
31. Review and approve the deployment plan for updates and patches for desktop assets.		X
32. Produce and submit all test documentation.	X	
33. Review and approve all test documentation.		X
34. Physically connect End-User Services Assets to the network.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
35. Provide technical support to End-Users for Incident activities.	X	
36. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices).	X	
37. Produce and submit to County all deployment documentation for End-User Services.	X	
38. Review and approve all deployment documentation for End-User Services.		X
39. Conduct deployment reviews and provide results to County.	X	
40. Review and approve results of deployment reviews.		X
41. Ensure that desktop technicians have the tools necessary to improve Incident resolution time and handle all Service Requests or IMARs.	X	

End-User Services Roles and Responsibilities		
42. Provide priority support for designated County High Response End-Users.	X	
43. Perform routine preventive maintenance according to the County approved preventative maintenance plans.	X	
44. Regularly review asset data and failure trends and develop plans to review and proactively repair the equipment.	X	
45. Perform predictive maintenance according to the County approved proactive repair plans.	X	
46. Provide quarterly report on Incidents based on desktop issues that includes a plan to resolve the top three issues.	X	
47. Install and configure any Hardware or Software needed to make Unified Communication and Messaging Services operational.	X	
48. Procure and own End-User Assets (e.g., Hardware, Software, operating system, personal productivity and office automation software, applicable warranty support).	X	
49. Deploy and manage End-User asset Hardware and Software	X	
50. Perform End-User Services optimization (e.g., performance, diagnostics and recovery).	X	
51. Deploy and manage Network-attached printers, storage devices and miscellaneous peripherals.	X	
52. Procure locally attached printers, storage devices and miscellaneous peripherals.	X	
53. Own locally attached printers, storage devices and miscellaneous peripherals.		X
54. Deploy and manage locally attached printers, storage devices and miscellaneous peripherals.	X	
55. Provide Tier 2 and Tier 3 support for Software as coordinated through the Service Desk.	X	
56. Provide Incident and Tier 2 support as coordinated through the Service Desk.	X	
57. Act as the interface to the Original Equipment Manufacturer (OEM) for warranty service on behalf of the County and/or act as a certified service agent and perform the service directly.	X	
58. Conduct warm transfer and/or follow-up and coordination with the OEM.	X	

4.5. Desktop Computing Services

4.5.1. Overview

This section pertains to the Desktop Computing Services Framework Component within the End-User Services Framework. The Desktop Computing Services Framework Component applies to all Hardware, Software and labor needed to maintain and support Desktop Computing Services for End-Users. Desktop Computing Services consist of activities associated with the Plan, Build and Operate of standard Hardware and Software used to support End-User Services.

4.5.2. High Level Requirements

4.5.2.1. Contractor shall provide standardization across the Desktop Computing Services Framework Component for all Hardware and Software.

4.5.2.2. Contractor shall deploy standard core software on all Desktop Computing Services Hardware.

4.5.2.3. Contractor shall recommend annually, for County approval, standards that support the End User Services.

4.5.2.4. Contractor shall ensure that each Desktop Computing Hardware recommended standard shall be available from the manufacturer for the entire Contract Year.

4.5.2.5. Contractor shall implement new Desktop Computing Hardware standards effective at the start of each Contract Year.

4.5.2.6. Contractor shall hard drive encrypt all Desktop Computing Hardware throughout the entire life-cycle.

4.5.2.7. Contractor shall ensure all Desktop Computing Hardware are installed with the defined core software standard.

4.5.2.8. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and

transformational activities related to operational and technical improvements of Desktop Computing Services.

4.5.2.9. Contractor shall provide Desktop Computing performance management consisting of measuring, modeling, planning, optimizing and reporting of Desktop Computing Services to ensure they operate with the speed, reliability and capacity to meet the needs of the County.

4.5.2.10. Contractor shall provide continuous desktop optimization to maximize response time for all County End-Users interactions with Portfolio Applications.

4.5.2.11. Contractor shall continuously maintain a timeline/roadmap of all Desktop Computing 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 assist in defining the standards.

4.5.2.12. Contractor shall provide Electronic Signature Services through a reliable and secure interface to allow County users to electronically share documents with external entities for review and eSigning via web browser. Electronic documents may be signed by external entities, County staff or both.

The Electronic Signature Services shall include:

- Electronic signature and associated digital signature management
- Service Desk support
- User administration
- Electronic signature service upgrade support
- eSigner authentication support
- WORD tagging support
- Template and workflow support
- eSigned document download support
- Monthly report for e-sign transactions

4.5.2.13. Contractor shall provide the Duo Hardware Token MFA to allow County employees and partners secure access, with Multi Factor Authentication (MFA), to the County network.

4.5.3. Environment

The following sub-sections further describe and scope Desktop Computing Services elements supported by Contractor and with which Contractor shall comply.

4.5.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Desktop Computing Services.

4.5.3.2. Desktop - Standard Workstation

4.5.3.2.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.2.2. All Desktop - Standard Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.2.3. All Desktop - Standard Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.3. Desktop - Advanced Workstation

4.5.3.3.1. All Desktops - Advanced Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.3.2. All Desktops - Advanced Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.4. Desktop - Advanced Engineering Workstation

4.5.3.4.1. All Desktops - Advanced Engineering Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.4.2. All Desktops - Advanced Engineering Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.5. Desktop - Engineering Workstation

4.5.3.5.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.5.2. All Desktops - Engineering Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.5.3. All Desktops - Engineering Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.6. Desktop - 3D Workstation

4.5.3.6.1. All Desktop – 3D Workstations shall be refreshed within a 3-year cycle from initial installation.

4.5.3.6.2. All Desktop – 3D Workstations shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.7. Laptop - Standard

4.5.3.7.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.7.2. All Laptop - Standard assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.7.3. All Laptop - Standard assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.8. Laptop - Ultra-Portable

4.5.3.8.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.8.2. All Laptop - Ultra-Portable assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.8.3. All Laptop - Ultra-Portable assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.9. Laptop - Engineering

4.5.3.9.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.9.2. All Laptop - Engineering assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.9.3. All Laptop – Engineering assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.10. Laptop - Ruggedized

4.5.3.10.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.10.2. All Laptop - Ruggedized assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.10.3. All Laptop - Ruggedized assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.11. Laptop – Standard LTE

4.5.3.11.1. All Laptop – Standard LTE shall be refreshed within a 3-year cycle from initial installation.

4.5.3.11.2. All Laptop – Standard LTE shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.12. Tablet - Ruggedized

4.5.3.12.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.12.2. All Tablet - Ruggedized assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.12.3. All Tablet – Ruggedized assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.13. Tablet - Convertible

4.5.3.13.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.13.2. All Tablet - Convertible assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.13.3. All Tablet Convertible assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.14.Desktop Scanner

4.5.3.14.1. All Desktop Scanners shall be refreshed within a 4-year cycle from initial installation.

4.5.3.14.2. All Desktop Scanners shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.15.Desktop - Mini Workstation

4.5.3.15.1. All Desktop - Mini Workstation shall be refreshed within a 4-year cycle from initial installation.

4.5.3.15.2. All Desktop - Mini Workstation shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.16.Desktop - Engineering Workstation Gold

4.5.3.16.1. All Desktop - Engineering Workstation Gold shall be refreshed within a 4-year cycle from initial installation.

4.5.3.16.2. All Desktop - Engineering Workstation Gold shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.17.Tablet – Surface Pro LTE

4.5.3.17.1. All Tablet-Surface Pro LTE shall be refreshed within a 3-year cycle from initial installation.

4.5.3.17.2. All Tablet-Surface Pro LTE shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.18.Desktop - Small Form Factor with Optical Drive

4.5.3.18.1. All Desktop - Small Form Factor with Optical Drive shall be refreshed within a 4-year cycle from initial installation.

4.5.3.18.2. All Desktop – Small Form Factor with Optical Drive shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.4. Early Refresh

The County may request early refresh of Desktop Computing asset. Early refresh is determined as refresh of the Desktop Computing asset; if the asset is not within 6 months of the scheduled refresh date. County shall request early refresh via a Service Request.

4.5.5. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Desktop Computing Services.

Desktop Computing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit all Desktop Computing Hardware and non-Hardware standards on an annual basis.	X	
2. Review and approve Desktop Computing Hardware standards.		X
3. Produce and submit yearly Desktop Computing Hardware refresh plan.	X	
4. Review and approve yearly Desktop Computing Hardware refresh plan.		X
5. Recommend and submit Desktop Computing software deployment/management policies and procedures.	X	
6. Review and approve Desktop Computing software deployment/management policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Deploy Legacy Provider desktop standards that were in effect as of the Service Framework Transition date during the first Contact Year.	X	
8. Develop core software image for Desktop Computing based on approved standards.	X	
9. Test standard core software image for Desktop Computing prior to deployment based on approved standards.	X	
10. Review results of test and approve deployment for the core software image for Desktop Computing.		X

Desktop Computing Services Roles and Responsibilities		
11. Deploy approved core software image to all Desktop Computing Assets.	X	
12. Provide staging Services for Desktop Computing at non-County Locations.	X	
13. Deploy and manage Desktop Computing Hardware and Software (e.g., operating system, personal productivity and office automation software and Services).	X	
14. Deploy software (e.g., patches, applications, drivers and operating systems) using a Contractor provided electronic software distribution tool.	X	
15. Provide a rapid response team during software deployment for assisting affected End-Users in the event a deployed package adversely affects End-Users or any systems.	X	
16. Deploy, manage, communicate and report activities related to Desktop Computing refresh.	X	
17. Review and approve reports for Desktop Computing refresh.		X
18. Develop and provide training related to the implementation of new products and services.	X	
19. Refresh all Desktop Computing Assets no later than 2 months after the expiration of a 3-year or 4-year cycle from initial installation, whichever is applicable.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
20. Provide support, including break-fix, for all Desktop Computing.	X	
21. Implement revised new desktop hardware standards so that they become effective at the start of each Contract Year.	X	
22. Encrypt hard drive of all Standard Desktops throughout the entire life cycle of the asset.	X	
23. Provide IMAR Services.	X	
24. Conduct data, End-User profile (e.g., favorites, bookmarks, MS Outlook profile) and Application migration that are necessary due to any Desktop Computing refresh, IMAR or Incident activity.	X	
25. Provide support for Desktop Computing refresh.	X	

Desktop Computing Services Roles and Responsibilities		
26. Provide core software updates, OIC software installation and new software releases for Desktop Computing Assets.	X	
27. Provide each End-User orientation on operational concepts of the new Desktop Computing at time of deployment.	X	
28. Provide and submit End-User tip sheets on such items as log on procedures, networked drives, system usage, core software, data storage and other practices that are essential to daily tasks.	X	
29. Review and approve End-User tip sheets prior to deployment.		X
30. Continually utilize automated Integrated Asset Management System tools to identify unlicensed software on desktops and servers and to pinpoint desktop devices not running the most recent antivirus software stipulated County standards and policies.	X	

4.6. Core Software Services

4.6.1. Overview

This section pertains to the Core Software Services Framework Component within the End-User Services Framework. The Core Software Services Framework Component describes the baseline, standard software installed on all Desktop Computing Assets, County Retained Assets, and other Computing Assets determined applicable by the County.

4.6.2. High Level Requirements

4.6.2.1. Contractor shall provide standardization of Core Software Services across all Desktop Computing Assets, County Retained Assets and other Computing Assets determined applicable by the County.

4.6.2.2. Contractor shall continuously maintain currency of core software standards deployed within the Desktop Computing Services Framework Component.

4.6.2.3. Contractor shall make recommendations for County approval of Core Software standards annually.

4.6.2.4. Contractor shall present and discuss Core Software standards at the County/Contractor Enterprise Architecture Governance.

4.6.2.5. Contractor shall publish Core Software standards in the Standards and Procedures Manual on the Service Portal.

4.6.2.6. Contractor shall refresh Core Software to latest standards annually for all Desktop Computing Assets and Retained Assets.

4.6.2.7. Contractor shall maintain currency, at all times, of Core Software deployed within the Desktop Computing Services and Retained Assets.

4.6.2.8. Contractor shall ensure all Desktop Computing Assets shall be deployed with the current standard Core Software.

4.6.2.9. Contractor shall ensure that there is no degradation of performance on all Core Software installed hardware.

4.6.2.10. Contractor shall ensure that optimal network performance on all Core Software installed hardware.

4.6.2.11. Contractor shall develop automated deployment strategies for Core Software installation on all hardware.

4.6.2.12. Contractor shall recommend annually, for County approval, standards that support the Core Software Services.

4.6.2.13. Contractor shall leverage all existing license agreements when recommending annual Core Software standards.

4.6.2.14. Contractor shall provide Core Software standards recommendations and submit for County approval.

4.6.2.15. Contractor shall ensure all Core Software is fully tested with all Desktop approved software to ensure the highest degree of operational integrity.

4.6.2.16. Contractor shall promptly patch and maintain all Core Software to the highest operational level throughout each Contract Year.

4.6.2.17. Contractor shall make effective new Core Software standards at the start of each Contract Year.

4.6.2.18. Contractor shall promptly update all Desktop Computing Assets to the latest Core Software standards annually or as the Core Software standards change.

4.6.2.19. Contractor shall maintain a timeline/roadmap of all Core Software Services software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Core Software that assists in defining the standards.

4.6.3. Environment

4.6.3.1. Software

Contractor shall supply all software to support Core Software Services.

4.6.4. Department of Child Support Services (DCSS) Core Software

The DCSS Core Software complies with the County Core Software standards with the following addition:

- INFO Connect version 4.1

4.6.5. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Core Software Services.

Core Software Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit annually core software standards for Desktop Computing Assets.	X	
2. Review and approve core software standards annually for Desktop Computing Assets.		X

Core Software Services Roles and Responsibilities		
3. Recommend and submit core software deployment/management policies and procedures.	X	
4. Review and approve core software deployment/management policies and procedures.		X
5. Develop a technical life cycle roadmap for each item in Core Software Services.	X	
6. Review and approve the technical life cycle roadmap for each item in Core Software Services.		X
7. Maintain all Core Software with the latest release version on all Desktop Computing Assets as defined in the approved standard.	X	
Build Roles and Responsibilities	**Contractor**	**County**
8. Maintain the same level of approved Core Software at all times for all Desktop Computing Assets.	X	
9. Develop core software image for Desktop Computing Assets based on approved standards.	X	
10. Test standard core software image for Desktop Computing Assets prior to deployment based on approved standards to ensure operational integrity.	X	
11. Review results of test and approve deployment for the core software image for Desktop Computing Assets.		X
12. Deploy approved Desktop Computing core software image.	X	
13. Engineer the core software image and provide any and all version changes, upgrades, enhancements, and additions to the core software image, to ensure that the core software image shall function properly on the desktop and the Applications Portfolio.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide support, including break-fix, for all Core Software Incidents.	X	
15. Provide Core Software updates, OIC software installation and new software releases for Desktop Computing Assets.	X	
16. Provide each End-User orientation on operational concepts of the new Core Software features and functions at time of deployment.	X	
17. Provide and submit End-User tip sheets on Core Software to the Service Portal.	X	

Core Software Services Roles and Responsibilities		
18. Continuously update all Core Software items including, latest patches, service releases, on all Desktop Computing Assets.	X	

4.7. County Retained Assets Services

4.7.1. Overview

This section pertains to the County Retained Assets Services Framework Component within the End-User Services Framework. County Retained Assets definition is Desktop Computing Services standard hardware purchased by the County and supported by the Contractor.

4.7.2. High Level Requirements

4.7.2.1. Contractor shall document, deliver (for County approval) and post to the Service Portal enrollment procedure for County Retained Assets.

4.7.2.2. Contractor shall document all County Retained Assets in the Integrated Asset Management System.

4.7.2.3. Contractor will maintain and support all County Retained Assets currently enrolled.

4.7.2.4. Contractor shall install standard Core Software on all County Retained Assets.

4.7.2.5. Contractor shall install the standard Core Software or DCSS Core Software for DCSS retained assets as determined by End-User Service Request.

4.7.2.6. Contractor shall exclude County Retained Assets from Desktop Computing Services refresh.

4.7.2.7. Contractor shall maintain Core Software to approved standards on County Retained Assets.

4.7.2.8. Contractor shall report to End-User the end of life of the County Retained Asset annually.

4.7.2.9. Contractor shall not exclude any County Retained Asset from the Services.

4.7.3. Environment

4.7.3.1. Hardware

The standard Desktop Computing Services Assets, published in the Standards and Procedures manual, are in scope for County Retained Assets Services.

4.7.3.2. Desktop - DCSS

4.7.3.2.1. All Desktop - DCSS owned by the State are Retained Assets.

4.7.3.2.2. All Desktop - DCSS shall follow the DCSS Core Software standards.

4.7.3.2.3. Contractor shall perform hardware refreshes for the Desktop - DCSS.

4.7.3.2.4. Desktop – DCSS will be refreshed every four years.

4.7.3.2.5. Contractor shall be responsible for IMARs, break-fix, and disposal of Desktop - DCSS in coordination with DCSS and the State.

4.7.3.3. Laptop – DCSS

4.7.3.3.1. Laptop – DCSS owned by the State shall be treated as County Retained Assets.

4.7.3.3.2. Laptop – DCSS shall follow the DCSS Core Software standards.

4.7.3.3.3. Laptop – DCSS refresh cycle shall be completed no later than 6 months after State provisioning.

4.7.3.3.4. Laptop refresh cycle shall begin upon the receipt of the initial laptop shipment from the State.

4.7.3.3.5. Contractor shall be responsible for IMARs, break-fix, and disposal for Laptop – DCSS in coordination with DCSS and the State.

4.7.3.4. Enrollment Requirements

Enrollment of County Retained Assets requirements are as follows:

- For new enrollment, the County Retained Assets must be compliant with current Desktop Computing Services hardware standards
- County Service Request is issued to initiate the enrollment process
- Contractor shall verify the requirements to enroll County Retained Assets

4.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with County Retained Assets Services.

County Retained Assets Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans for use of the Integrated Asset Management System to track Retained Assets.	X	
2. Review and approve plans for use of the Integrated Asset Management System to track Retained Assets.		X
3. Ensure that DCSS Retained Assets comply with the DCSS Core Software standards.	X	
Build Roles and Responsibilities	**Contractor**	**County**
4. Validate during enrollment, that the new Retained Assets are compliant with current Desktop Computing Services standards.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
5. Provide support, including break-fix, for all County Retained Assets Incidents.	X	
6. Provide hardware support for all County Retained Assets.	X	
7. Maintain and update the County Retained Assets inventory.	X	
8. Maintain and support County Retained Assets currently enrolled at the time of Transition.	X	
9. Tag Retained Assets with a Contractor's asset tag in addition to the existing County property tag and track these in the Integrated Asset Management System.	X	

County Retained Assets Services Roles and Responsibilities		
10. Verify Retained Asset enrollment requirements and submit to County for review and approval.	X	
11. Review and approve Retained Asset enrollment requirements.		X
12. Perform the Retained Asset enrollment.	X	
13. Install current Core Software Standard County Retained Assets.	X	
14. Install the current Core Software Standard or DCSS Core Software for DCSS Retained Assets.	X	
15. Perform hardware refresh of each DCSS Retained Assets in accordance with the State refresh standards.	X	
16. Provide IMARs, break-fix, and disposal of DCSS Retained Assets in coordination with DCSS and the State.	X	

4.8. Mobile Device Support Services

4.8.1. Overview

This section pertains to the Mobile Device Services Framework Component within the End-User Services Framework. The Mobile Device Services Framework Component applies to providing support to County End-Users in the operational and business use of County owned Mobile Devices which include Retained Assets and authorized BYOD. Mobile Device Services consist of activities associated with the Plan, Build and Operate of managed mobile devices and bring-your-own mobile devices (BYOD).

4.8.2. High Level Requirements

4.8.2.1. Contractor shall provide Service Desk Services support and End-User Services support for supported County owned Mobile Devices.

4.8.2.2. Contractor shall support End-User Mobile Devices as requested by a Service Request. Contractor shall consider this optional support.

4.8.2.3. Contractor shall enable and support connectivity for a supported Mobile Device to County resources.

4.8.2.4. Contractor shall assist End-Users with the operational use of supported Mobile Devices.

4.8.2.5. Contractor shall continuously provide, update and maintain documentation, FAQs and other related tip sheets to County End-Users via the Service Portal.

4.8.2.6. Contractor shall support End-User authentication to County resources for all supported Mobile Devices.

4.8.2.7. Contractor shall provide Incident tracking, escalation and resolution for supported Mobile Devices.

4.8.2.8. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of supported Mobile Devices.

4.8.2.9. Contractor shall continuously develop, update and maintain Service Desk scripts and processes for Mobile Device Support Services End-User support.

4.8.2.10. Contractor shall continuously update instructions, FAQs and other documentation for End-Users on the Service Portal.

4.8.2.11. Contractor shall support BYOD devices as specified in County policy.

4.8.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Mobile Device Support Services.

Mobile Device Support Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Implement mobile device support Services per the approved procedures.	X	

Mobile Device Support Services Roles and Responsibilities		
2. Produce and submit recommendations (on annual basis) the Mobile Device supportable assets standards.	X	
3. Review and approve all Mobile Device supportable assets standards recommendations.		X
4. Review and approve standardization across the managed Mobile Device Services Framework Component for all mobile hardware and software.		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Provide enterprise mobile device application store support.	X	
6. Manage County-approved BYOD devices and the installed County-approved applications on such devices.	X	
7. Deploy or remove mobile applications using the Enterprise Application Store.	X	
8. Perform device password resets as required.	X	
9. Assist End-Users with any Incidents or Incidents arising from application releases and patches.	X	
10. Coordinate Incident and Service Request resolution among End-Users, the Service Desk and Third-Parties to manage all End-User MDM related Incidents and Service Requests as needed.	X	
11. Troubleshoot and resolve access Incidents to authorized enterprise content from any authorized mobile device.	X	
12. Monitor and report the usage of self-service for mobile devices.	X	
13. Produce and submit mobile device support solutions that best meet County business needs and security policies.	X	
14. Review and approve mobile device support solutions.		X
15. Produce and submit End-User instructions on provisioning and configuration of mobile devices.	X	
16. Review and approve End-User instructions on provisioning and configuration of mobile devices.		X

Mobile Device Support Services Roles and Responsibilities		
17. Manage mobile Users enrollment and access by Active Directory (AD) group membership.	X	

4.9. Unified Communications Services

4.9.1. Overview

The Unified Communications Services Framework Component within the End-User Services Framework applies to the process allowing County End-Users to communicate efficiently and effectively through various integrated methods. Unified Communications Services provide strategy, process, methodology, support and documentation Real-Time or Non Real-Time methods deployed to End-User Services.

Real-Time methods are, but not limited to, instant messaging (IM), presence, voice, mobility, audio, desktop web & video conferencing, desktop sharing, data sharing, interactive whiteboards, call control.

Non Real-Time methods are, but not limited to, integrated voice mail, E-Mail, SMS and fax.

4.9.2. High Level Requirements

4.9.2.1. Contractor shall provide Service Desk Services support and End-User Services support for Unified Communications Services.

4.9.2.2. Contractor shall support End-User authentication to County resources for all Unified Communications Services.

4.9.2.3. Contractor shall provide, upon County approval, Unified Communications Services externally (off County network).

4.9.2.4. Contractor shall provide Incident tracking, escalation and resolution for Unified Communications Services.

4.9.2.5. Contractor shall support BYOD devices as specified in County policy for Unified Communications Services.

4.9.2.6. Contractor shall provide standardization across the Unified Communications Services client software.

4.9.2.7. Contractor shall be own, provision, maintain, update and support all Hardware and Software associated with providing Unified Communications Services.

4.9.2.8. Contractor shall deploy to all Desktop Computing Assets, Retained Assets and mobile devices client software needed to engage in Unified Communications Services.

4.9.2.9. Contractor shall maintain at all times, current standard version of Unified Communications Services client software to all Desktop Computing Assets, Retained Assets and mobile devices.

4.9.2.10. Contractor shall provide Incident tracking, escalation and resolution for Unified Communications Services.

4.9.2.11. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Unified Communications Services.

4.9.2.12. Contractor shall continuously develop, update and maintain help desk scripts and processes for Unified Communications Services End-User support.

4.9.2.13. Contractor shall recommend, for County approval, Unified Communications Services client software standards annually.

4.9.3. Environment

4.9.3.1. All Desktop Computing Services Assets shall be supported for Unified Communications Services.

4.9.3.2. All County owned and managed mobile devices shall be supported for Unified Communications Services.

4.9.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Unified Communications Services.

Unified Communications Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Unified Communications Services policies and procedures.	X	
2. Review and approve Unified Communications Services policies and procedures.		X
3. Recommend (on annual basis) the Unified Communications Services standards.	X	
4. Review and approve the recommended Unified Communications Services standards.		X
5. Develop and submit recommended standardization across the managed Unified Communications Services.	X	
6. Review and approve standardization across the managed Unified Communications Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Perform the installation, testing, and tuning of all technical environment Hardware, Software, peripherals and interfaces related to the support of Unified Communications Services platforms.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Perform end-to-end Incident determination and resolution for all Unified Communications Services related Incidents.	X	
9. Provide and support Remote Access Services for Unified Communications Services for defined County resources.	X	
10. Take corrective action as needed for all Unified Communications Services.	X	
11. Coordinate Incident resolution with Technical Support, Incident & Problem Management and Third-Parties.	X	
12. Provide troubleshooting, repair and escalation of Incidents within the Unified Communications Services platform environment.	X	

Unified Communications Services Roles and Responsibilities		
13. Provide End-User training, tip sheets, FAQs and post to the Service Portal.	X	
14. Perform Incident support activities as required, remotely or on-site.	X	
15. Provide Tier 2 and 3 technical assistance and support for Unified Communications Services End-Users.	X	

4.10. Catalog Services

4.10.1. Overview

Catalog Services Framework Component of End-User Services consist of activities associated with Optional Item Catalog (OIC). The OIC contains the Hardware and Software items that are approved for the End-User Services environment; consisting of distinct categories of goods and services available for purchase by the County.

4.10.2. High Level Requirements

4.10.2.1. Contractor shall promptly publish the current OIC in the Standards and Procedures Manual as changes occur.

4.10.2.2. Contractor shall make available the updated and current OIC within the Service Request system.

4.10.2.3. Contractor shall acquire, configure, deliver, install and support OIC items throughout their useful life.

4.10.2.4. Contractor shall maintain, as changes occur, the published OIC.

4.10.2.5. Contractor shall recommend, for County approval, changes to the OIC.

4.10.2.6. Contractor shall maintain currency of all items in the OIC with recommendations to the County.

4.10.2.7. Contractor shall meet all IMAR Service Level obligations for all items in the OIC.

4.10.2.8. Contractor shall provide recommended updates, for County approval, to the OIC based on Desktop Computing Services standards.

4.10.2.9. Contractor shall provide recommend software packages that comply with Core Software standards.

4.10.2.10. Contractor shall acquire, configure, deploy, support and maintain all OIC items delivered to End-Users throughout the useful like of the OIC item.

4.10.2.11. Contractor shall configure, deploy, support and maintain, as needed, Portfolio Application client software needed for End-Users business functions.

4.10.2.12. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Catalog Services and the OIC.

4.10.2.13. Contractor shall continuously develop, update and maintain help desk scripts and processes for Catalog Services End-User support.

4.10.2.14. Contractor shall continuously maintain a timeline/roadmap of all OIC Hardware and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of Hardware and Software that assist in defining the standards.

4.10.3. Environment

The OIC categories of components are segmented and distinct categories. These categories offer organization and definition to the OIC. These segmented and distinct categories are as follows:

Desktop Peripheral Hardware	Hardware physically connected to a Desktop Computing asset, including, but not limited to, printers, scanners,

	keyboards, managed mobile devices and monitor upgrades.
Stand-Alone Hardware	Hardware that is not physically connected to a Desktop Computing asset Including, but not limited to, videoconferencing optional equipment, audio/video equipment, and replacement parts.
Desktop Software	Classified in accordance with the Desktop Applications Directory (DAD). Includes acquisition, license management, engineering, deployment, rights management, and full maintenance of the software by the Contractor. The County shall manage the DAD, including adds, deletes, and updates of approved Applications on the list.
Portfolio Application Client Software	Portfolio Application client software not otherwise covered by a Resource Unit (i.e., Non-DAD Commercial Off-the-Shelf ("COTS") Software).
IT Training Courses	IT Training Courses as needed to support County business needs and enterprise license agreements.

4.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Catalog Services:

Catalog Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define, add, modify and delete Hardware and Software items in Optional Item Catalog (OIC).		X
2. Produce and submit recommendations for updates to Hardware and Software items in the OIC.	X	
3. Review and approve updates to Hardware and Software items in the OIC.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Maintain currency of items in the OIC.	X	

Catalog Services Roles and Responsibilities		
5. Host and make available the OIC to County Users on a proven table-driven catalog management system.	X	
6. Organize the OIC to facilitate ordering and viewing for End-Users.	X	
7. Publish the OIC on the Service Portal, with online help functions, for viewing and ordering.	X	
8. Provide all engineering necessary to ensure functionality of all Hardware and Software items in the OIC with Desktop Computing Assets.	X	
9. Test all new and updated Hardware and Software items listed in the OIC prior to deployment.	X	
10. Develop and submit a deployment plan for any multi-End-User OIC implementations.	X	
11. Review and approve deployment plan for any multi-End-User OIC implementations.		X
12. Publish all new and updated items in the OIC at the conclusion of the engineering activity.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Authorize items to be included in OIC.		X
14. Add or modify the DAD listed in the OIC via a Service Request.	X	
15. Maintain and support (as listed in the "Level of Support" section of the OIC), including break-fix, all Software and Hardware in the OIC.	X	
16. Provide IMAR Services for OIC items.	X	
17. Maintain and publish on a monthly basis the OIC.	X	
18. Provide Web access and ordering abilities for the OIC to all County End-Users.	X	
19. Provide ongoing OIC User training.	X	
20. Provide End-User orientation on operational concepts of new Hardware or Software installed via order from the OIC.	X	
21. Review new manufacturers' product posted offerings, verify the currency of the listed equipment, and maintain the accuracy of the OIC.	X	

4.11. Network Printer Services

4.11.1. Overview

This section pertains to the Network Printer Services Framework Component within the End-User Services Framework. The Network Printer Services Framework Component applies to all Hardware, Software and back-end infrastructure needed to maintain and support networked Printer Assets. Network Printer Services consist of the activities associated with the Plan, Build and Operate of all networked Printer Assets.

4.11.2. High Level Requirements

4.11.2.1. Contractor shall provide recommend standards, for County approval, annually for Network Printer Services.

4.11.2.2. Contractor shall provide a redundant, highly available, and technical current back-end infrastructure to support Network Printer Services.

4.11.2.3. Contractor shall deploy and manage back-end infrastructure that is redundant with complete fail-over minimizing any associated print service Incident.

4.11.2.4. Contractor shall maintain currency on all print drivers used to deliver the Network Printer Services.

4.11.2.5. Contractor shall maintain currency, at all times, of Network Printer Assets firmware.

4.11.2.6. Contractor shall determine, with County approval, categories of Network Printer Assets.

4.11.2.7. Contractor shall ensure that each Network Printer recommended standard be available from the manufacturer for the entire Contract Year.

4.11.2.8. Contractor shall publish in the OIC the standards for Network Printer Services.

4.11.2.9. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Network Printer Services.

4.11.2.10. Contractor shall continuously develop, update and maintain help desk scripts and processes for Network Printer Services End-User support.

4.11.2.11. Contractor shall leverage existing license agreements to the extent possible for all Network Printer Services.

4.11.2.12. Contractor shall make effective new Network Printer standards at the start of each Contract Year.

4.11.2.13. Contractor shall supply, via Service Portal, a list of consumables, updated annually or as standards change, for current printers deployed to County End-Users in the environment.

4.11.2.14. Contractor shall exclude Printers not attached or connected to the County network.

4.11.2.15. County shall be responsible for Network Printer consumables which are defined as paper and ink/toner.

4.11.2.16. Contractor shall be responsible for all maintenance and availability, including break-fix, of Network Printer Services.

4.11.2.17. Contractor shall maintain and update annually a timeline/roadmap of all Core Software versions and life cycles to adequately plan timeframes and completion dates to stay within supported versions.

4.11.3. Environment

4.11.3.1. Hardware

The County current Network Printer standards fall into the following categories:

- Monochrome Network Workgroup Printer — Standard Format (abbreviated as "MNWP")
- Monochrome Network Workgroup Printer — Large Format (11x17) (abbreviated as "MNWP-LF")
- Monochrome Network High Volume Printer — Large Format (11x17) (abbreviated as "MNWP-LF-H")
- Color Network Workgroup Printer — Large Format (abbreviated as "CNWP-LF")
- Color Network Workgroup Printer — Standard Format (abbreviated as "CNWP")

4.11.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Printer Services.

Network Printer Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit Network Printer Assets policies, procedures and Hardware standards on an annual basis.	X	
2. Review and approve Network Printer Assets policies, procedures and hardware standards.		X
3. Produce and submit the annual Network Printer asset refresh plan.	X	
4. Review and approve the annual Network Printer asset refresh plan.		X
5. Provide standardization across the Network Printer Services Framework Component for all Hardware and Software.	X	
Build Roles and Responsibilities	**Contractor**	**County**
6. Determine which multifunction or specialized printer devices shall be purchased.	X	
7. Review and approve the purchase of the multifunction or specialized printer devices.		X
8. Provide network connectivity and print queue installation for County purchased. Such devices shall be reviewed with Contractor prior to selection.	X	

Network Printer Services Roles and Responsibilities		
9. Provide staging Services for Network Printer Assets at non-County locations.	X	
10. Deploy and manage Network Printer Hardware and Software (e.g., printer drivers).	X	
11. Deploy, manage, communicate and report activities related to Network Printer refresh.	X	
12. Review and approve reports for Network Printer refresh.		X
13. Identify the IT Coordinator for each deployed Network Printer prior to transition or deployment.	X	
14. Develop and provide training related to the implementation, use and operation of Network Printers.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
15. Perform the Network Printer hardware asset refresh not later than two months after the expiration of the four-year cycle.	X	
16. Provide support, including break-fix, for all Network Printer Assets.	X	
17. Provide Network Printer IMAR Services.	X	
18. Provide support for Network Printer Assets refresh.	X	
19. Provide printer driver updates.	X	
20. Provide each departmental IT coordinator orientation on operational concepts of the new printer asset at time of deployment.	X	
21. Order and replace toner cartridges and paper from County office supply sources.	X	

4.12. Electronic File Sharing and Synchronization Services

4.12.1. Overview

This section pertains to the Electronic File Sharing Services (EFSS) component within the End User Services Framework. The Electronic File Sharing Services Framework Component applies to all Hardware, Software and labor needed to maintain and support EFFS.

4.12.2. High Level Requirements

4.12.2.1. Contractor shall provide, maintain and support a centralized, secure EFSS with access through browsers on approved and managed County computing devices.

4.12.2.2. Contractor shall provide EFSS with granular permissions to protect confidential, sensitive and public information that may be posted.

4.12.2.3. Contractor shall provide EFSS that allows County users to share and collaborate on files internally and externally.

4.12.2.4. Contractor shall provide EFSS that allows external users to consume or share files to and/or from County users.

4.12.2.5. Contractor shall provide standard County single sign-on for authenticating County Active Directory users.

4.12.2.6. Contractor shall provision County users to access EFSS as per authorized Service Request.

4.12.2.7. Contractor shall provide County users with the ability to create temporary secure locations for sharing files that are too large for email. The temporary secure location shall be accessible to County users and external users with access expiring after designated time period as set by sharing party or after twenty-four (24) hours, whichever is less.

4.12.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with EFFS.

Electronic File Sharing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Implement EFFS as per approved procedures.	X	
2. Produce and submit plans for updates/upgrades to EFSS.	X	

Electronic File Sharing Services Roles and Responsibilities		
3. Review and approve plans for updates/upgrades to EFSS.		X
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide onboarding support for EFSS.	X	
5. Provide, update and maintain documentation, FAQs and other related tip sheets to County End Users via the Service Portal.	X	
6. Assist End Users with any Incidents associated with EFSS.	X	
7. Maintain and support EFSS. This includes maintaining all the integration points (e.g., Single Sign On, Content Delivery Network services), break-fix, etc.	X	
8. Provide IMAR Services for EFSS.	X	
9. Provide operational reports for EFSS.	X	

4.13. Audio/Video (A/V) Conference Rooms Services

4.13.1. Overview

This section pertains to the A/V Conference Rooms Installation Services Framework Component within the End User Services Framework. The A/V Conference Rooms Services Framework Component applies to the installation and support for Audio/Video Conference Rooms.

4.13.2. High Level Requirements

4.13.2.1. Contractor shall provide three (3) standardized Audio/Video Conference Rooms Services:

a. A/V Conference Room - Small

b. A/V Conference Room - Medium

c. A/V Conference Room - Large

4.13.2.2. Audio/Video Conference Rooms Services shall include the following:

- Equipment
- Equipment installation
- 3-year System support

The above items are defined in Exhibit 4.3-2 Audio/Video Conference Rooms Configuration and Support.

4.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Audio/Video Conference Rooms Services.

Audio/Video Conference Rooms Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Submit request to initiate Audio/Video Conference Rooms installation indicating Conference Room size.		X
2. Produce and submit plans for Audio/Video Conference Rooms installation.	X	
3. Review and approve plans for Audio/Video Conference Rooms installation.		X
4. Produce and submit procedures for Audio/Video Conference Rooms installation.	X	
5. Review and approve procedures for Audio/Video Conference Rooms installation.		X
Build Roles and Responsibilities	**Contractor**	**County**
6. Design and implement Audio/Video Conference Rooms installation.	X	
7. Approve design and implementation of Audio/Video Conference Rooms installation.		X
Operate Roles and Responsibilities	**Contractor**	**County**
8. Support Audio/Video Conference Rooms as defined in Exhibit 4.3-2 Audio/Video Conference Rooms Configuration and Support.	X	

4.14. Digital Signage Services

4.14.1. Overview

This section pertains to the Digital Signage Services Framework Component within the End User Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- Automatically download text, images and other content from websites
- Extract data in multiple formats
- Connect and Control screens over the internet
- Send extracted data to specified location

4.14.2. High Level Requirements

4.14.2.1. Contractor shall procure Digital Signage subscription services and/or devices.

4.14.2.2. Contractor shall renew Digital Signage subscriptions services with County approval.

4.14.2.3. Contractor shall provide installation, incident support, escalation, and resolution for Digital Signage Services.

4.14.2.4. Contractor shall replace a defective Digital Signage device within the warranty period.

4.14.2.5. Contractor will provide for purchase, via the OIC, Digital Signage services and/or devices.

4.14.3. Environment

The following further describe, and scope Digital Signage Services elements supported by Contractor and with which Contractor shall comply.

4.14.3.1. Hardware and Software

Contractor shall provide all devices, needed to provide the Digital Signage Services as offered by Third Party.

4.14.3.2. Technology Upgrade and Refresh

Digital Signage devices supported within the Digital Signage Services are eligible for refresh or upgrade on a three-year subscription cycle and provided for purchase, via the OIC.

4.14.4. Roles and Responsibilities

Digital Signage Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide Digital Signage Services recommendations and specifications.	X	
2. Review and approve Digital Signage Services recommendations and specifications.		X
3. Develop IMAR and Incident process flows for Digital Signage Services.	X	
4. Develop OIC plans for approved Digital Signage Services.	X	
5. Provide OIC information for Digital Signage Services.	X	
6. Review and approve plans for Digital Signage Services processes.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Implement Digital Signage Services inventory process.	X	
8. Implement Digital Signage Services device warranty management.	X	
9. Implement Help Desk scripts for Digital Signage Services issues.	X	
10. Deploy OIC offerings for Digital Signage Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
11. Provision Digital Signage Services as ordered by the County.	X	
12. Provide IMAR and Incident services for Digital Signage Services.	X	
13. Manage Asset Management database of Digital Signage Services for warranty and upgrade/refresh purposes.	X	
14. Provide in-warranty Digital Signage Services devices replacement as needed.	X	
15. Provide for on-site Digital Signage Services for incidents.	X	

4.15. Reserved.

4.16. Survey Solution Support Services

4.16.1. Overview

This section pertains to the Survey Solution Support Services component within the End User Services Framework. Survey Solution is designed to collect, assess, and share survey responses.

4.16.2. High Level Requirements

4.16.2.1. Contractor shall migrate existing County users based upon County-approved plan.

4.16.2.2. Contractor shall migrate existing survey data based upon County-approved plan.

4.16.2.3. Contractor shall provide Service Desk support services, including for external users.

4.16.2.4. Contractor shall be responsible for managing Administrative Users per authorized Service Requests. Administrative Users control the workgroups, create subdivisions of such workgroups, invite County Casual Users, and control the sharing of data across workgroups. Administrative Users must have an sdcounty.ca.gov email address.

4.16.2.5. Contractor shall allow for an unlimited number of Casual Users. Casual Users have view/collaboration privileges only as subordinate to one or more Administrative Users and can send surveys with less than 10 questions.

4.16.2.6. Contractor shall be responsible for managing top-level workgroups per authorized Service Requests.

4.16.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Survey Solution Support Services.

Survey Solution Support Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop plan for County review for implementation, operations, and support, including (but not limited to) asset management, incident management, Service Portal updates, annual procurement support, user and data migration activities, workgroup definitions and activities, documentation, required integration points, required reporting, etc.	X	
2. Review implementation, operations, and support, including (but not limited to) asset management, incident management, Service Portal updates, annual procurement support, user and data migration activities, workgroup definitions and activities, documentation, required integration points, required reporting, etc.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Responsibility to execute the Implementation portion of the Plan developed in the Plan R&R.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Responsibility to execute the Support portion of the Plan developed in the Plan R&R.	X	

5. NETWORK SERVICES

5.1. Overview

Network Services Framework includes the Hardware, Software and services associated with the transport of voice, video and/or data across the infrastructure, internet, data centers, and cloud based services and/or external Third-Parties to/from End-Users. Activities included are the plan, build, and operate of networked assets and services used for the transport of voice, video and/or data.

Network Services Framework includes the following Framework Components:

- Data Network Services
- Remote Access Services
- Voice Services
- Network Security Services
- Video Conferencing Services
- Video Streaming and Archiving Services
- Mobility Infrastructure Services
- Wireless Network Access Services
- Third-Party Network Access Services
- External DNS Management Services
- IP Address Management Services
- New Site Installation Services

5.2. High Level Requirements

5.2.1. Contractor shall recommend, for County approval, qualified Network Service Manager as Contractor Key Personnel to manage Network Services.

5.2.2. Contractor shall provide a reliable, scalable, responsive and secure data network with connectivity to all Locations.

5.2.3. Contractor shall provide highly available, scalable, reliable, and secure voice services with features and functions that meet or exceed County business requirements.

5.2.4. Contractor shall continuously improve Network Services.

5.2.5. Contractor shall provide all Network Services across, at a minimum, two Point of Presence locations within the County that maintains complete failover and redundancies for all Network Services.

5.2.6. Contractor shall implement a dedicated, secure, high capacity, and redundant backbone with County defined bandwidth that shall be dual homed across the two Point of Presence Locations.

5.2.7. Contractor shall provide redundant, secure, diverse Internet connections for County End-Users at each Point of Presence location.

5.2.8. Contractor shall ensure County business continues to operate during any unplanned event or outage.

5.2.9. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Network Services.

5.2.10. Contractor shall continuously investigate emerging technology and services that improve the overall network efficiencies, lowers overall network costs and improves End-User network performance and security.

5.2.11. Contractor shall provide technology assistance and support to the County in planning and standardsetting activities.

5.2.12. Contractor shall maintain a secure network perimeter.

5.2.13. Contractor shall provide secure network remote access to County End-Users and authorized Third-Parties.

5.2.14. Contractor shall provide bandwidth, as County deems necessary, to accommodate the County needs and for the Services.

5.2.15. Contractor shall measure and report bandwidth consumption across all Network Services.

5.2.16. Contractor shall incorporate technology security improvements for business requirements without compromising the security, integrity, and performance of the County enterprise and information resources.

5.2.17. Contractor shall refresh and consolidate network assets to ensure operability, supportability and performance.

5.2.18. Contractor shall continuously identify and correct, with County approval, any single point failures found within Network Services.

5.2.19. Contractor shall perform centralized management and performance monitoring of Network Services.

5.2.20. Contractor shall provide network bandwidth as needed to meet County performance and operational requirements.

5.2.21. Contractor shall ensure that all Sites have sufficient bandwidth, at all times, to support the Services.

5.2.22. Contractor shall ensure that all Network Services Hardware and Software are operating at optimal and maximum performance.

5.2.23. Contractor shall report performance and capacity results monthly on Network Services.

5.2.24. Contractor shall ensure that all Network Services Hardware and Software related to network security are physically located in secure Locations.

5.2.25. Contractor shall interconnect all Sites to facilitate endtoend business functions and allow network access to shared resources.

5.2.26. Contractor shall maintain a timeline/roadmap of all Network 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.

5.2.27. Contractor shall configure, install, activate, monitor and provide break-fix support to County for equipment and circuits funded through the E-Rate Program, as agreed to and defined in the Standards and Procedures (SnP) Manual for the San Diego County Branch Libraries.

5.3. Environment

5.3.1. Scope of Environment

Network Services shall cover all County Locations.

5.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Network Services.

5.3.3. Facilities

5.3.3.1. County

Network Services for all County Locations.

5.3.3.2. Contractor

Network Services for Contractor Locations used by the Contractor to provide the Services.

5.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Services.

Network Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Collaborate with Third-Party network carriers and other industry leaders on an initial and ongoing basis to develop and establish the most favorable, cost-effective strategic direction for voice technology for the County.	X	
2. Produce and submit network architecture documentation.	X	
3. Review and approve network architecture documentation.		X
4. Produce and submit network asset refresh plan.	X	
5. Review and approve network asset refresh plan.		X
6. Produce and submit capacity and trending analysis for network infrastructure.	X	
7. Review and approve capacity and trending analysis for network infrastructure.		X
8. Produce and submit impact analyses and associated plans.	X	
9. Review and approve impact analyses and associated plans.		X

Network Services: Plan, Build and Operate Roles and Responsibilities		
10. Produce and submit standards for network cable plant to include wiring standards, fiber standards, terminations, faceplates, cable run, and cable type.	X	
11. Review and approve standards for network cable plant to include wiring standards, fiber standards, terminations, faceplates, cable run, and cable type.		X
12. Produce and submit recommendations on maintaining the network cable plant to industry standard.	X	
13. Review and approve recommendation on maintaining the network cable plant to industry standard.		X
14. Produce and submit plans for Site additions or deletions upon request.	X	
15. Review and approve plans for Site additions or deletions upon request.		X
16. Recommend network capacity thresholds.	X	
17. Approve network capacity planning thresholds.		X
18. Provide consulting for strategy and direction including architecture consultative support.	X	
Build Roles and Responsibilities	**Contractor**	**County**
19. Design and implement network architecture based on approved documentation.	X	
20. Design, configure, deploy and report network assets based on the approved refresh plan.	X	
21. Review and approve network asset refresh plan.		X
22. Design and implement changes to the network infrastructure based on results of the capacity and trending analysis.	X	
23. Design and implement changes to the network infrastructure based on impact analyses and associated plans.	X	
24. Design and implement approved recommendations on maintaining the network cable plant to industry standard.	X	
25. Implement network cable plant standards.	X	

Network Services: Plan, Build and Operate Roles and Responsibilities		
26. Design and implement network devices to meet County availability requirements (e.g., ensure that critical servers such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory, E-Mail, etc. have dual-attached network interface cards (NICs) to independent LAN switches and/or have backup servers).	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Provide maintenance and support for all Network Services, including the cable plant, network hardware and circuits.	X	
28. Perform proactive 24/7/365 network monitoring and maintenance functions for all Framework Components (e.g., voice systems, video systems, and data network transport) from County-approved network operations centers (NOC).	X	
29. Manage all network devices in accordance with County's policies (including security oversight and change management policies).	X	
30. Manage User accounts as needed for access and maintaining network resources (e.g., logon User-id and password maintenance).	X	
31. Maintain and provide verified information including access, general logs, application logs in accordance with County's security policies.	X	
32. Ensure that network administration activities are coordinated through defined change management processes.	X	
33. Support and manage network cable plant to approved standards.	X	
34. Provide updates to network Standards documentation as required.	X	
35. Synchronize all network device time clocks using appropriate tools that meets county requirements (e.g., Network Time Protocol (NTP)).	X	
36. Backup network device configurations.	X	
37. Review and approve Services and standards for all network Services.		X
38. Respond and resolve data network-related Incidents.	X	
39. Provide management of hardware refresh activities for network infrastructure.	X	

Network Services: Plan, Build and Operate Roles and Responsibilities		
40. Manage and perform refresh of Network hardware per County standard hardware refresh cycles.	X	

5.5. Data Network Services

5.5.1. Overview

This section pertains to the Data Network Services Framework Component within the Network Services Framework. The Data Network is the transport layer of a converged network with voice, video and data communications coexisting seamlessly.

Services provided within this Framework Component include, but are not limited to, the following:

- Network management
- Network capacity and performance monitoring
- Site to site connectivity
- Bandwidth management
- End-User to network connectivity
- Network engineering
- Internet access
- Hardware and Software refresh
- Technology transformation to improve overall service delivery
- Uninterrupted Power Supply (UPS) equipment support

5.5.2. High Level Requirements

5.5.2.1. Contractor shall maintain currency on Data Network Services Hardware and Software.

5.5.2.2. Contractor shall maintain an accurate and up-to-date inventory of all Data Network Services Hardware and Software.

5.5.2.3. Contractor shall standardize, with County approval, all Hardware and Software used in the delivery of Data Network Services.

5.5.2.4. Contractor shall provide bandwidth, as needed, for all Data Network Services, including the Internet, in support of the Services.

5.5.2.5. Contractor shall provide continuous monitoring and corrective action of the Data Network Services, 24/7/365.

5.5.2.6. Contractor shall participate in continuous architecture planning of upgrades, refresh and transformational activities related to operational and technical improvements of Data Network Services.

5.5.2.7. Contractor shall design all Wide-Area-Networks (WAN) with requirements for cloud connectivity.

5.5.2.8. Contractor shall continuously assess network impact of County adoption of cloud based services.

5.5.2.9. Contractor shall participate in County cloud review committee.

5.5.2.10. Contractor shall centralize the management of Data Network Services including cloud activity.

5.5.2.11. Contactor shall include cloud services in Service Levels.

5.5.2.12. Contractor shall provide network performance management consisting of measuring, modeling, planning, optimizing and reporting of Data Network Services to ensure they carry traffic with the speed, reliability and capacity to meet the needs of the County.

5.5.2.13. Contractor shall manage network performance by continuously measuring delay, packet loss, retransmissions, and throughout.

5.5.2.14. Contractor shall promptly correct and reported performance or capacity Incidents with Data Network Services.

5.5.2.15. Contractor shall perform monitoring and break/fix support and break/fix support of Contractor provided UPS equipment.

5.5.2.16. Contractor shall perform active and passive techniques for measuring and analyzing network performance as needed to support Incident Management and Problem Management.

5.5.3. Environment

The following further describe and scope Data Network Services elements supported by the Contractor and with which Contractor shall comply.

5.5.3.1. Technology Refresh

Contractor shall refresh Data Network Services core hardware and software on a 4-year refresh schedule and Data Network Services LAN Switch hardware and software on a 5-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.5.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of services for Data Network Services.

5.5.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Data Network Services.

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendation for Data Network Services architecture.	X	
2. Review and approve recommendations for Data Network Services architecture.		X
3. Produce and submit Data Network Services refresh plan on a yearly basis.	X	
4. Review and approve Data Network Services refresh plan on a yearly basis.		X
5. Identify, recommend and submit Data Network Services solutions that best meet County business needs.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
6. Review and approve Data Network Services.		X
7. Perform and submit recommendations for Data Network Services capacity and performance policies and procedures.	X	
8. Review and approve recommendations for Data Network Services capacity and performance policies and procedures.		X
9. Produce and submit recommendations for Data Network Services migration to current technology.	X	
10. Review and approve recommendations for Data Network Services migration to current technology.		X
11. Produce and submit operational policies and procedures for monitoring and maintaining Data Network Services.	X	
12. Review and approve operational policies and procedures for monitoring and maintaining Data Network Services.		X
13. Produce and submit network provisioning policies and procedures.	X	
14. Review and approve network provisioning policies and procedures.		X
15. Produce and submit network administration policies and procedures.	X	
16. Review and approve network administration policies and procedures.		X
17. Produce and submit documentation of Data Network Services asset configuration files and IP addressing schemas.	X	
18. Review and approve documentation of Data Network Services asset configuration files and IP addressing schemas.		X
Build Roles and Responsibilities	**Contractor**	**County**
19. Produce and submit to County all design and engineering documentation to support Data Network Services.	X	
20. Review and approve all design and engineering documentation for Data Network Services.		X
21. Design, test and implement approved Data Network Services architecture.	X	
22. Deploy, manage, communicate and report on activities related to Data Network Services refresh.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
23. Review and approve Data Network refresh report.		X
24. Design and Implement Data Network Services capacity and performance policies and procedures.	X	
25. Design, test and implement Data Network Services migration to current technology.	X	
26. Implement operational policies and procedures for monitoring and maintaining Data Network Services.	X	
27. Design and implement network provisioning policies and procedures.	X	
28. Implement approved recommendations for Sites additions or deletions.	X	
29. Implement approved network administration policies and procedures.	X	
30. Order and expedite WAN circuits, Assets and Services.	X	
31. Configure Data Network Assets prior to installation.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
32. Provide support, including break-fix, for all Data Network Services.	X	
33. Manage public carriers and other circuit Third-Parties to ensure delivery of WAN Services.	X	
34. Monitor Data Network Services to established baseline and thresholds.	X	
35. Provide and support Data Network Services refresh.	X	
36. Provide and support Data Network Services migration to new technology or architecture.	X	
37. Produce and submit Data Network Services utilization, capacity and performance reports monthly.	X	
38. Review and approve requirements for WAN/LAN/VPN/Firewall Services.		X
39. Provide LAN/WAN connectivity to Locations.	X	
40. Manage and support provisioning of new and upgraded Data Network Services.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
41. Procure, provision and maintain all network components and circuits.	X	
42. Provide support in accordance with approved network administration policies and procedures.	X	
43. Perform day-to-day network operations and administration activities.	X	
44. Maintain TCP/IP addressing schemes, router configurations, routing tables, VPN configurations, network addresses, MAC addresses, etc.	X	
45. Support legacy data networks and associated terminals, controllers and CSU/DSU, tied to current mainframe and midrange platforms.	X	
46. Manage LAN infrastructure, including wiring, patch panels, jack configuration and documentation.	X	
47. Implement measures for proactive monitoring and self-healing to limit network Incidents.	X	
48. Identify network Incidents and resolve in accordance with Incident Management Services.	X	
49. Perform and support physical (e.g., equipment) and logical (e.g., IP address change) IMAR associated with Sites for LAN/WAN and transport environments.	X	
50. Manage the performance of public carriers (and other Third-Parties) to meet defined schedules, Project plans, and performance.	X	
51. Coordinate ordering, procurement and inventory management of network circuits from public carriers.	X	
52. Perform point-to-point and promiscuous network traffic analysis.	X	
53. Provide monitoring and break/fix support for Contractor supplied UPS equipment.	X	

5.6. Remote Access Services

5.6.1. Overview

This section pertains to the Remote Access Services Framework Component within the Network Services Framework. Services provided by this Framework Component include,

but are not limited to, the provision of a persistent, secure, and wireless connection to internal County-networked Hardware, Software and applications from outside the County network perimeters for authorized End-Users on a 24/7/365 basis.

Services provided within this Framework Component include, but are not limited to, the following:

- VPN
- Mobile VPN
- Akamai Enterprise Application Access (EAA)
- Network persistence
- Application persistence
- Network access control
- Application tunneling
- External and mobile authentication
- Active directory account integration
- Integration with the County certificate authority
- Technology refresh

5.6.2. High Level Requirements

5.6.2.1. Contractor shall maintain a safe, reliable and secure session that allows County End-Users and authorized external Users access to designated County network resources.

5.6.2.2. Contractor shall continuously identify and correct, with County approval, any single point failures with Remote Access Services.

5.6.2.3. Contractor shall provide network persistence as part of the Remote Access Services and shall be referred to as Virtual Private Network Level 1.

5.6.2.4. Contractor shall provide application persistence as part of the Remote Access Services and shall be referred to as Virtual Private Network Level 2.

5.6.2.5. Contractor shall provide network access control (NAC) to all Remote Access Services.

5.6.2.6. Contractor shall apply County approved security policies to all Remote Access Services.

5.6.2.7. Contractor shall provide End-User Authentication for all Remote Access Services.

5.6.2.8. Contractor shall provide secure application tunneling or similar HTTP/SSL tunneling technology for County End-Users.

5.6.2.9. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Remote Access Services.

5.6.2.10. Contractor shall develop training documentation and End-User FAQs and post it on the Service Portal for County End-Users.

5.6.2.11. Contractor shall develop, use, maintain and update help desk scripts and processes for Remote Access Services End-User support.

5.6.2.12. Contractor shall provide secure, external facing portal access to County applications for approved End-Users.

5.6.3. Environment

The following further describe and scope Remote Access Services elements supported by Contractor and with which Contractor shall comply.

5.6.3.1. Technology Refresh

Contractor shall refresh Remote Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.6.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools and Akamai Enterprise Application Access cloud services needed in the delivery of Remote Access Services.

5.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Remote Access Services.

Remote Access Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for a consolidated Remote Access Services architecture.	X	
2. Review and approve recommendations for Remote Access Services architecture.		X
3. Produce and submit operational policies and procedures for Remote Access Services.	X	
4. Review and approve operational policies and procedures for Remote Access Services.		X
5. Produce and submit plans for updates and patches to Remote Access Services.	X	
6. Review and approve plans for updates and patches to Remote Access Services Assets.		X
7. Produce and submit Remote Access Services reporting requirements.	X	
8. Review and approve Remote Access Services reporting requirements.		X
9. Recommend Remote Access Services Desktop Application.	X	
Build Requirements, Roles and Responsibilities	**Contractor**	**County**
10. Design, test and implement County-approved Remote Access Services.	X	
11. Design and implement County-approved operational policies and procedures for Remote Access Services.	X	
12. Design, test and implement approved plans for updates and patches to Remote Access Services.	X	
Operate Requirements, Roles and Responsibilities	**Contractor**	**County**

Remote Access Services: Plan, Build and Operate Roles and Responsibilities		
13. Provide support, including break-fix, for all Remote Access Services Assets.	X	
14. Maintain, support and report on Remote Access Services.	X	
15. Review and approve report on Remote Access Services.		X
16. Maintain and support County Locations requiring Remote Access Services.	X	
17. Maintain and support approved operational policies and procedures.	X	

5.7. Voice Services

5.7.1. Overview

This section pertains to the Voice Services Framework Component within the Network Services Framework. The Voice Services Framework Component applies to Hardware and Software needed to operate the telecommunications systems within the County.

Services provided within this Framework Component include, but are not limited to, the following:

- Single and multi-line voice services
- Single and multi-line Voice over Internet Protocol (VoIP) services
- Voice Mail
- Local dial plans
- Long distance plans
- Voice mail to E-Mail
- Basic and Simple Interactive Voice Services
    - Basic and Simple Interactive Voice Service are defined as the support for Auto Attendant and Automated Call Distributor services as a right to use feature within Voice Services. Functionality is inherent to the Avaya enterprise voice network.
- Auto Attendants
- Automated Call Distribution (ACD)
- Analog jacks
- Short Messages Services

- Telephone handsets
- IP Conference Phones
- 4-1-1 operator Services
- Virtual Phone

5.7.2. High Level Requirements

5.7.2.1. Contractor shall interconnect all Locations along a common voice network to facilitate end-to-end business functions, reduce toll calls and lower costs.

5.7.2.2. Contractor shall provide Voice Services as a highly converged and highly redundant part of Network Services.

5.7.2.3. Contractor shall utilize SIP trunking internally and externally to provide cost optimization and network efficiency for Voice Services.

5.7.2.4. Contractor shall continuously maintain technical currency and modernization of Voice Services.

5.7.2.5. Contractor shall deploy VOIP services to all new County Sites.

5.7.2.6. Contractor shall, on Service Request, upgrade County Site to VOIP services.

5.7.2.7. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Voice Services.

5.7.2.8. Contractor shall provide Voice Mail Services that can be transcribed and delivered to County End-User E-Mail as requested by the County.

5.7.2.9. Contractor shall continuously identify and correct, with County approval, any single point failures with Voice Services.

5.7.2.10. Contractor shall develop plan, implement and integrate Unified Communication Services into Voice Services.

5.7.2.11. Contractor shall develop plan, implement and integrate Voice Services onto Desktop Computing Services Assets.

5.7.2.12. Contractor shall implement, maintain and support basic and simple IVS systems.

5.7.2.13. Contractor shall recommend a plan for County approval, and execute the approved plan for changes to continuously reduce County usage costs for Voice Services.

5.7.2.14. Contractor shall deploy and maintain VoIP Services to appropriate quality of service.

5.7.2.15. Contractor shall enable a Switched Ethernet connection (Power over Ethernet (POE)) for VoIP Services.

5.7.2.16. Contractor shall continuously provide and update documentation that details operation and use VoIP services and post them on the Service Portal Users.

5.7.2.17. Contractor shall recommend, for County approval, technology and architectural standards on a yearly basis for all Voice Services.

5.7.3. Environment

The following further describe and scope Voice Services elements supported by Contractor and with which Contractor shall comply.

5.7.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Voice Services.

5.7.3.2. Technology Refresh

Contractor shall refresh Voice Services Hardware and Software on a 5-year refresh schedule unless otherwise agreed by the County in writing, and at a

County-approved deployment schedule that minimizes disruption and reduces risk.

5.7.3.3. Single-Line Voice Services

Single-Line Voice Services are all the Hardware, Software and services necessary to provide single-line phone services to End-Users.

5.7.3.4. Multi-Line Voice Services

Multi-Line Voice Services are all the Hardware, Software and services necessary to provide multi-line phone services to End-Users.

5.7.3.5. Single VoIP Services

Single-Line VoIP Services are all the Hardware, Software and services necessary to provide single-line VoIP Services to End-Users.

5.7.3.6. Multi-Line VoIP Services

Multi-Line VoIP Services are all the Hardware, Software and services necessary to provide multi-line VoIP Services to End-Users.

5.7.3.7. Voice Mail

Voice Mail is an available option to Voices Services upon End-User Service Request or as a stand-alone option available to End-Users without a phone.

The second available option is voice-to-text conversion for Voice Mail. The appropriate E-Mail address receives the converted voice message. This option requires an End-User Service Request.

5.7.3.8. Analog Jack

Analog Jacks are available upon End-User Service Request.

5.7.3.9. [Reserved]

5.7.3.10.Telephone Handsets

Contractor shall own, provision, install, manage, maintain, and support all telephone handsets, including VOIP, with the exclusion of the Microsoft Teams Phone handsets.

5.7.3.11.Virtual Phone

Virtual Phone Services are all the Hardware with the exclusion of the Microsoft Teams Phone handsets., Subcontractor Software, Third Party Software (other than Third Party Software provided by Contractor), and services necessary to provide Virtual Phone Services to End-Users.

5.7.3.12 Virtual Phone Advanced Features

Virtual Phone Services – Advanced Features is an available option to Virtual Phone - Microsoft (MS) Teams Phone and provides auto attendant and call queues. These Advanced Features are only available to MS Teams – Phone subscribers.

5.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Voice Services.

Voice Service: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Voice Services solutions that best meets County business requirements.	X	
2. Review and approve recommended Voice Services solutions that best meet County business requirements.		X
3. Produce and submit a VOIP migration plan.	X	
4. Review and approve VOIP migration plan.		X
5. Produce and submit operational plans for Voice Services capacity and performance management.	X	
6. Review and approve operational plans for Voice Services capacity and performance policies and procedures.		X
7. Produce and submit recommendations for Voice Services architecture.	X	
8. Review and approve recommendations for Voice Services architecture.		X
9. Produce and submit Voice Services refresh plan on a yearly basis.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
10. Review and approve Voice Services refresh plan on a yearly basis.		X
11. Produce and submit recommendations for Voice Services migration to current technology.	X	
12. Review and approve recommendations for Voice Services migration to current technology.		X
13. Produce and submit operational policies and procedures for management and support of Voice Services.	X	
14. Review and approve operational policies and procedures for management and support of Voice Services.		X
15. Provide Desk Phone design and engineering to meet County requirements.	X	
16. Approve Desk Phone design and engineering.		X
17. Develop Voice and Web Conferencing Services strategies and requirements.		X
18. Consult on Voice, Web Conferencing Service and Desk Phone strategies with County and actively assist in planning and strategy.	X	
19. Design Voice and Web Conferencing Services to meet County strategies and requirements.	X	
20. Approve Voice and Web Conferencing Services.		X
21. Design and implement customized call flow.	X	
22. Design all queues based on customer requirement that provide Agent mobility.	X	
23. Provide call flow and queue design documentation to each Business Group.	X	
24. Provide consultation to County in developing new or modifying existing ACD applications.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
25. Collaborate with Third-Parties and analyze the following traffic analysis and call reports: • 800 in-bound network traffic summary report • Call detail hourly summary • Call detail traffic summary • Report by each 800 number • Call detail traffic summary by state • Trunk utilization for all trunk groups • Call detail by location • Call completion analysis • Resellers summarized traffic by number • Call prompter summary • Traffic by number and date • Unassigned routing termination number (RTN) • Dial number by RTN	X	
Build Roles and Responsibilities	**Contractor**	**County**
26. Design, test and implement approved Voice Services solutions that best meet County business requirements.	X	
27. Provide least cost routing (LCR) analysis and PBX technology that provides LCR (e.g., "tail end-hop off" LCR methodology).	X	
28. Implement approved operational plans for Voice Services capacity and performance management.	X	
29. Design, test and implement Voice Services architecture.	X	
30. Deploy, manage, communicate and report on activities related to Voice Services refresh.	X	
31. Review and approve Voice refresh report.		X
32. Design, test and implement Voice Services migration to current technology.	X	
33. 33. Install Direct Routing between the O365 Microsoft Teams Tennant and on-premise Avaya Aura infrastructure.	X	
34. Implement approved operational policies and procedures for management and support of Voice Services.		X
Operate Roles and Responsibilities	**Contractor**	**County**
35. Provide support, including break-fix, for all Voice Services Assets.	X	
36. Perform bandwidth management for Voice Services.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
37. Support Voice Services refresh.	X	
38. Support Voice network optimization and traffic engineering.	X	
39. Provide competitive and economically favorable local and long distance rates.	X	
40. Manage and provide end-to-end internal and external phone connectivity including hardware and/or peripherals.	X	
41. Provide Desk Phone requirements (e.g., number of sets, functions and features).		X
42. Assist with set up, troubleshooting, and recommendations on headset options.	X	
43. Provide and maintain End-User Guides, quick reference guides, VoIP training, and End-User Telecom Tips/Q&A for County to publish.	X	
44. Manage PBX systems for class of service according to the authorized County key personnel.	X	
45. Manage the PBX systems to provide least cost routing and tail end hop off for outbound calls.	X	
46. Manage interfaces between PBX network and public carriers.	X	
47. Manage and support Interactive Voice Services.	X	
48. Provide emergency 911 Services to County phones.	X	
49. Provide adaptive voice telecommunications Services and equipment as required by laws affecting the support of the disabled.	X	
50. Manage and maintain private dial plan to be consistent with the County's current dialing method.	X	
51. Provide local and long distance voice Services.	X	
52. Support and manage long distance telephone calling.	X	
53. Provide local and long distance usage monitoring and reporting.	X	
54. Provide and support analog jacks for equipment such as modems, fax machines, or phones.	X	
55. Provide Voice Mail Services.	X	
56. Manage Voice Mail security PBXs, Voice Mail systems, and other Voice Services Assets.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
57. Provide Voice Mail usage monitoring and reporting.	X	
58. Provide Voice Mail storage capacity management.	X	
59. Provide Voice Mail retention management per County requirements and external regulations.	X	
60. Perform Voice Mail mailbox IMARs.	X	
61. Maintain Voice Mail mailboxes configurations by End-User.	X	
62. Provide new Voice Mail End-User training materials.	X	
63. Provide access to voice messages through County E-Mail system.	X	
64. Provide directory Services to the public through a mix of automated and live operators in order to meet call requirements.	X	
65. Provide a secure and searchable online directory service with real time updates (e.g., global directory facility GDF).	X	
66. Provide 411 operator Services for the County which includes a directory of employees, employee locations, departments and telephone numbers.	X	
67. Maintain a directory of County Services for 411 operator Services.	X	
68. Provide 411 operator Services for employee and public inquiries.	X	
69. Update annually telephone numbers.	X	
70. Maintain and update an employee directory website with data from County systems.	X	
71. Maintain business process, systems, and information for phone book and directory assistance in accordance with County approved system design and business processes.	X	
72. Manage local, intrastate, national and international voice teleconferencing Services and support.	X	
73. Provide support for the setup of Voice and Web Conferencing sessions.	X	
74. Create and maintain a monthly and a year-to-date summary report by host, including: conference types, total number of connects, total number of minutes, total call charges, total feature charges, and total charges.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
75. Provide proactive and reactive Voice Services fraud and security management and reporting.	X	
76. Monitor and record all data, such as call rating tables, call usage detail and Move, Add, and Remove orders, generate cost allocation reports for local and long distance usage as well as completed Move, Add and Remove orders.	X	
77. Provide itemized call detail records, including length of each call by telephone number and charge.	X	
78. Provide, maintain and support tollfree (on-net) calls between all County Locations.	X	
79. Provide Casual Use Calling including collect calls, person-to-person calls, person-to-person collect calls, remote calls, operator assistance calls, Third-Party calls, dial one calls, dedicated calls and other miscellaneous calls.	X	
80. Provide Conference Bridge Calls for calls placed to an audio and Web document sharing conference Services that allow multiple people participation and controlled by a unique access code.	X	
81. Provide Directory Assistance Calls for calls placed to obtain a listed telephone directory number.	X	
82. Provide Pay Phones at County Sites for the public's convenience, upon End-User request.	X	
83. Provide an attempted (offered) and handled call volume summary.	X	
84. Provide duration, call transferred and abandoned call reports.	X	
85. Provide PSTN calling for toll free and toll calling as per Exhibit 16.1.1	X	
86. Maintain PSTN calling plan for Microsoft Teams Phone, Single-line Voice and Multi-line Voice RUs as per Exhibit 16.1.1.	X	
87. Operate and maintain Direct Routing between the O365 Microsoft Teams Tennant and on-premise Avaya Aura infrastructure	X	
88. Provide SMS text messaging through IVS applications.	X	
89. Provide IP Conference phones.	X	

5.8. Network Security Services

5.8.1. Overview

The Network Security Services Framework Component of the Network Services Framework includes the Hardware, Software, and services needed to maintain overall network and perimeter security.

Services provided by this Framework Component include, but are not limited to, the following:

- Protection from unauthorized devices, software or users
- Protection from unauthorized access to, or use of, the network and networked assets
- Firewall Services
- Intrusion protection, detection and reporting
- Cloud Access Security Broker (CASB)
- Network Access Control
- Remote Access and Mobile Device Authentication
- Remote Access and Mobile User Authentication
- Data Loss Prevention (DLP)
- Continuous security monitoring, logging and reporting
- Security architecture services
- Data protection
- Prevention of malicious code entry into the network
- Transformational activities to improve the overall security, increase performance and lower costs
- Web content filtering

5.8.2. High Level Requirements

5.8.2.1. Contractor shall develop and maintain a flexible security architecture.

5.8.2.2. Contractor shall provide protection from unauthorized use of, or access to, the County's network and networked resources.

5.8.2.3. Contractor shall control physical access to all Hardware and Software used to provide Network Services.

5.8.2.4. Contractor shall establish secure zones, with County approval, as needed.

5.8.2.5. Contractor shall lock down all Hardware and Software used for Network Services.

5.8.2.6. Contractor shall continuously scan all perimeters and assess vulnerabilities and risk.

5.8.2.7. Contractor shall increase visibility into all data communications and data flows between End-Users and resources within the Data Center or to cloud based services.

5.8.2.8. Contractor shall ensure necessary throughput for perimeter protection and internal security methods that are fast enough to deeply scan and remediate threats at wire speed.

5.8.2.9. Contractor shall implement a "single pane of glass" approach to management and monitoring of Network Security Services.

5.8.2.10. Contractor shall provide management, refresh, support, reporting and logging of all firewalls used in the delivery of the Services.

5.8.2.11. Contractor shall provide information event logging, analysis, reporting and management of all Hardware and Software used to provide Network Security Services.

5.8.2.12. Contractor shall provide intrusion detection and prevention systems.

5.8.2.13. Contractor shall provide unified threat management.

5.8.2.14. Contractor shall update all Hardware and Software used for Network Security Services to the latest patch, service packs, or other updates promptly to ensure operational integrity.

5.8.2.15. Contractor shall refresh all Hardware and Software used for Network Security Services on a 4-year cycle unless otherwise approved by the County.

5.8.2.16. Contractor shall maintain all Hardware used in the delivery of Network Security Services to maximize performance with high-speed network operations.

5.8.2.17. Contractor shall continuously identify and correct, with County approval, any single point failures within the Network Security Services.

5.8.2.18. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Network Security Services.

5.8.2.19. Contractor shall continuously maintain a timeline/roadmap of all Network Security Services Hardware and Software 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.

5.8.2.20. Contractor shall provide a cloud-based CASB service that will enforce County security policy on County SaaS data. This will include enforcement of DLP policies, enforcement of collaboration policies, capture of audit trails for forensic use, detection of compromised accounts and other threats, and other features that further extend the County security protection.

5.8.3. Environment

The following further describe and scope Network Security Services elements supported by Contractor and with which Contractor shall comply.

5.8.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Network Security Services

5.8.3.2. Technology Refresh

Contractor shall refresh Network Security Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.8.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Security Services.

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Security architecture.	X	
2. Review and approve recommendations for Security architecture.		X
3. Produce and submit plans for monitoring and managing access to the County Intranet.	X	
4. Review and approve plans for monitoring and managing access to the County Intranet.		X
5. Produce and submit plans that provide security to physical and logical devices connected to the network.	X	
6. Review and approve plans to include the provision and support of methods that provide security to physical and logical devices connected to the network.		X
7. Produce and submit recommendations on firewall policies that comply with County policy.	X	
8. Review, approve and identify firewall policies that comply with County policy.		X
9. Perform firewall engineering and firewall security design	X	
10. Assess firewall security and propose alternative security designs.	X	
11. Review and approve firewall security designs.		X
12. Produce and submit recommendation of Network Security Services Assets refresh or upgrade plan on a yearly basis.	X	
13. Review and approve recommendations on Network Security Services Assets refresh or upgrade plan.		X

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
14. Produce and submit recommendations for improved network security.	X	
15. Review and approve recommendations for improved network security.		X
16. Produce and submit recommendation of policies for security vulnerability and penetration testing.	X	
17. Review and approve policies for security vulnerability and penetration testing.		X
18. Produce and submit plans for Network Security Services asset updates or patches.	X	
19. Review and approve plans for Network Security Services asset updates or patches.		X
Build Roles and Responsibilities	**Contractor**	**County**
20. Design, test and implement approved Network Security architecture.	X	
21. Design and implement monitoring and managing access plans as approved.	X	
22. Design, test and implement plans to secure network attached devices.	X	
23. Design, test and implement approved firewall policies.	X	
24. Design, test, implement and report Network Security Services Assets refresh or upgrade.	X	
25. Review and approve reports for Network Security Services Assets refresh or upgrade.		X
26. Design and implement approved recommendations for improving network security.	X	
27. Design and implement approved policies for security vulnerability and penetration testing.	X	
28. Design, test and implement updates or patches approved for Network Security Services Assets.	X	
29. Design a centralized authentication database for remote County employees, Third-Party and agents using VPN and deploy new systems interfacing with single-sign-on authentication Services.	X	

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
30. Deploy a Security Information Management System (SIMS) for aggregation and centralization of Incident alerts and correlation and provide SIMS information to the County through online access.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
31. Provide support, including break-fix, for all Security Services Assets.	X	
32. Provide 24/7/365 security monitoring Services including a Security Operations Center (SOC), IDS/IPS infrastructure and intranet/Internet firewalls.	X	
33. Provide services in conformance to firewall policies and requirements.	X	
34. Provide reporting on security testing results.	X	
35. Provide initial review of security Incidents and the determination if escalation, including to County Information Security, is warranted.	X	
36. Provide standardized End-User operations and also custom reports regardless of the End-User's location and/or department.	X	
37. Identify and remove from the network any malicious-code infected System.	X	
38. Identify and provide countermeasures for malicious code attacks (i.e., both prevention and remediation).	X	
39. Block unauthorized party access and provide notification of unauthorized access attempts.	X	
40. Encrypt (and prioritize) all County traffic that uses public MPLS network transport facilities (such as OPT-E-MAN or DSL) through the engineering and implementation of generic routing encapsulation (GRE) VPN tunnels (e.g., 256-bit Advanced Encryption Standard (AES) key).	X	
41. Provide technical expertise for security reviews.	X	
42. Collect all logs and review all Incidents reported by all other security Services (e.g., NIPS, HIPS, penetration testing, and firewall).	X	
43. Maintain log files in accordance with County policies and Service Levels.	X	

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
44. Provide security reporting.	X	
45. Provide fraud prevention, detection and reporting.	X	
46. Provide, control, monitor, and maintain security encryption interface at the data network level.	X	
47. Provide security devices on supported PBXs, Voice Mail systems, and other appropriate adjunct remote administration ports.	X	
48. Implement security violation notification.	X	
49. Conduct security perimeter vulnerability assessments and annual penetration testing.	X	
50. Provide Cloud Access Security Broker (CASB) capability.	X	
51. Provide CASB reporting.	X	
52. Provide CASB connectivity to Contractor SIEM service.	X	

5.9. Video Conferencing Services

5.9.1. Overview

Video Conferencing Services Framework Component of the Network Services Framework consists of the activities and functions of providing two-way video transmission between different entities within the County as well as outside of the County.

Services provided by this Framework Component include, but are not limited to, the following:

- Enable closed-circuit video conference
- Point-to-point communications within County network connected Sites
- Point-to-point to external State or Federal facilities
- Multi-point hosting of meetings
- Desktop integration into Video Conferencing Services
- External multi-point integration into Video Conferencing Services
- Develop two types of Video Conferencing systems: room and personal.

5.9.2. High Level Requirements

5.9.2.1. Contractor shall provide a reliable and secure Video Conferencing Services that enables County End-Users and authorized external Users to participate.

5.9.2.2. Contractor shall identify and correct, with County approval, any single point failures with Video Conferencing Services.

5.9.2.3. Contractor shall integrate Unified Communications Services into Video Conferencing Services.

5.9.2.4. Contractor shall plan and implement, as requested by the County, Town Hall Services for internal County use.

5.9.2.5. Contractor shall apply County approved security policies to all Video Conferencing Services hardware, software and services.

5.9.2.6. Contractor shall provide End-User authentication, as needed, for all Video Conferencing Services.

5.9.2.7. Contractor shall continuously provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Video Conferencing Services.

5.9.2.8. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Video Conferencing Services.

5.9.2.9. Contractor shall continuously develop, update and maintain help desk scripts and processes for Video Conferencing Services End-User support.

5.9.3. Environment

The following further describe and scope Video Conferencing Services elements supported by Contractor and with which Contractor shall comply.

5.9.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Video Conferencing Services

5.9.3.2. Technology Refresh

Contractor shall refresh Video Conferencing Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.9.4. Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Video Conferencing Services.

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for video conferencing standards annually.	X	
2. Review and approve recommendations for video conferencing standards.		X
3. Publish video conferencing standards in the Standards and Procedures Manual on the Service Portal.	X	
4. Produce and submit plans for new, replacement and upgrades to Video Conferencing Services.	X	
5. Produce and submit plans for infrastructure systems (Gatekeeper and Border Controller) and network capacities to support IP based VTC systems.	X	
6. Review and approve plans for new, replacement and upgrades to Video Conferencing Services, infrastructure/network systems.		X
7. Provide Project Management for the installation of new VTC systems.	X	
8. Conduct site review to determine the installation time period (the installation interval is targeted to be 30 days or less, the actual installation period shall be determined after a site review is conducted for that particular system).	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
9. Review and approve site review report.		X
10. Make recommendations to the County for new Video Conferencing Services strategy as new devices, infrastructures and protocols emerge.	X	
11. Review and approve recommendations for new Video Conferencing Services strategy as new devices, infrastructures and protocols emerge.		X
12. Provide a selection of Video Conferencing Services optional items via the OIC.	X	
13. Select Video Conferencing Services optional items via the OIC.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Design and implement new, replacement or upgrades to Video Conferencing Services.	X	
15. Design and implement infrastructure systems to support IP based VTC systems.	X	
16. Review and approve design changes and implementation plans to Video Conferencing Services, infrastructure and network systems/circuits.		X
17. Provide infrastructure systems that monitors and maintains the QOS of the IP network (Gatekeeper) and supports secure off-net IP based video conferences (Border Controller).	X	
18. Provide basic installation which includes the assembly and placement of any furniture (roll-about cart), component or option provided as part of the new VTC system; along with the placement, connecting, configuration and testing of any electronics provided as part of the new VTC system and any other activities.	X	
19. Review and approve the installation activities.		X
20. Test and deploy approved changes to Video Conferencing Services including infrastructure systems and network Services.	X	
21. Develop and provide training related to the implementation of new products and Services.	X	
22. Provide training to County department personnel for proper operation of hardware and software components and scheduling tool.	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
23. Provide network access to new systems by trained and qualified video engineers and technicians to enable remote diagnostics and efficient triage of trouble reports.	X	
24. Provide Users access to the VTC Third-Party Supplier's management system scheduling tool so that County End-Users can schedule their own video conferences.	X	
25. Provide project management including coordinating with and providing support to Third-Party.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Provide support and maintenance, including break-fix, for new Video Conferencing Services, and limited break-fix for legacy Video Conferencing Systems (excluding parts replacement for legacy Video Conferencing Systems).	X	
27. Provide IMAR Services.	X	
28. Provide and support infrastructure Services for point-to-point, multipoint video conferencing, and Presentation features, Quality of Service and on-net/off-net video conferencing security.	X	
29. Support Video Conferencing Assets.	X	
30. Provide point-to-point, multi-point and ISDN to IP video conferencing Services to the County, both inside and outside the County's network.	X	
31. Provide and maintain the network security infrastructure to support external video conferences for all County departments.	X	
32. Provide video bridging service for County's use to facilitate IP and multipoint video conferences.	X	
33. Provide single point of contact for Incident call handling.	X	
34. Provide access to manufacturer's customer service technical support center to assist County End-Users on equipment operation and any other questions they may have about the systems.	X	
35. Provide software patches and version updates as recommended by equipment for Video Conferencing Services Assets.	X	
36. Provide parts and device warranty, repair and/or parts replacement of all components for systems of Video Conferencing Services.	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
37. Provide multi-cast record/archive service.	X	
38. Integrate teleconferencing into video conference meetings upon request.	X	
39. Monitor and support calls in progress.	X	
40. Maintain and manage video conference calendar and scheduling.	X	
41. Manage and maintain video room calendar and coordinate reservations.	X	
42. Provide miscellaneous video support and advice as required by County.	X	
43. Provide video conferencing service support through County Service Desk.	X	

5.10. Video Streaming and Archiving Services

5.10.1. Overview

This section pertains to the Video Streaming and Archiving Services Framework Component within the Network Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- providing live or archived video data or content via a web page to the County Intranet or the external public
- archiving such video data or content to be available for public viewing for one year

County currently uses Granicus Services to provide the Video Streaming and Archiving Services.

5.10.2. High Level Requirements

5.10.2.1. Contractor shall provide and maintain live video streaming broadcast, of Board of Supervisors meetings, over the Internet to worldwide audiences and to End-Users.

5.10.2.2. Contractor shall deliver and distribute video streaming broadcasts of high quality video to all End-Users.

5.10.2.3. Contractor shall provide and maintain video streaming across the County network.

5.10.2.4. Contractor shall optimize Video Streaming and Archiving Services across the County network to maximize End-User performance.

5.10.2.5. Contractor shall identify and correct and single point issues with the Video Streaming and Archiving Services to ensure maximum reliability and performance.

5.10.2.6. Contractor shall archive video streamed broadcasts and store such archives for twelve months and provide public access, via the Internet, to and viewing of such archives.

5.10.2.7. Contractor shall provide the Board of Supervisors with a solution to automate and easily manage the entire legislative process. In particular this solution will allow the elected officials to submit Board Letters, compiling and generating agendas, and creating Minute Orders.

5.10.2.8. Contractor shall provide a web-based service to collect feedback from citizens on specific items associated with upcoming Board of Supervisor's meetings. Contractor shall also provide an online solution that promotes and facilitates community engagement by allowing constituents to share opinions, submit questions, create polls and surveys.

5.10.2.9. Contractor shall provide a custom web page for collecting the feedback and such web page activated by a link dropped on the County's existing Board of Supervisors agenda page.

5.10.2.10. Contractor shall provide a touch-voting solution to the Board of Supervisors, which will include the following functionalities:

5.10.2.10.1. Real-time meeting voting and recording via touch-screen device such as the VoteCast Classic and an iPad or Android voting machine.

5.10.2.10.2. Viewing of full agendas and supporting materials via touch-screen.

5.10.2.11. Elected officials can make or second a motion, cast a vote, review previously cast votes, and request to speak on items using touch-screen devices.

5.10.2.12. Contractor will provide hosting services sufficient to enable use of, and access to, the application. Contractor will also provide maintenance and support of all hardware, firmware, software, and telecommunications equipment and facilities necessary for the delivery of the services.

5.10.2.13. Contractor shall continuously provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Video Streaming and Archiving Services.

5.10.2.14. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Video Streaming and Archiving Services.

5.10.2.15. Contractor shall continuously develop, update and maintain help desk scripts and processes for Video Streaming and Archiving Services End-User support.

5.10.3. Environment

The following further describe and scope Video Streaming and Archiving Services elements supported by Contractor and with which Contractor shall comply.

5.10.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Video Streaming and Archiving Services.

5.10.3.2. Technology Refresh

Contractor shall refresh Video Streaming and Archiving Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Video Streaming and Archiving Services.

Video Streaming and Archiving Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit annual plans and recommendations for new, replacement and upgrades to Streaming and Archiving Services based on market evaluation and emerging technologies.	X	
2. Review and approve annual plans and recommendations		X
Operate Roles and Responsibilities	**Contractor**	**County**
3. Provide support, including break-fix, for Video Streaming and Archiving Services.	X	
4. Provide and maintain internet video and audio streaming broadcasts, including broadcasts of Board of Supervisors meetings.	X	
5. Provide archiving and public viewing and retrieval of broadcasts of Board of Supervisors meetings for twelve (12) months following the date of such meetings.	X	
6. Provide broadcast feed of County of San Diego Board of Supervisors meetings to the Cox (or the applicable successor) cable television distribution network.	X	

5.11. Mobility Infrastructure Services

5.11.1. Overview

This section pertains to the Mobility Infrastructure Services Framework Component within the Network Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- Mobile device management

- Centralized mobile device management platform
- Manage mobile device configurations
- Provision device security policies
- Mobile device authentication services
- Mobile application store
- Application gateways
- Mobile VPN services

5.11.2. High Level Requirements

5.11.2.1. Contractor shall provide a reliable and secure Mobility Infrastructure Services for mobile County End-Users and authorized bring your own device (BYOD) Users.

5.11.2.2. Contractor shall design, deliver, for County approval, and implement a mobile device management platform.

5.11.2.3. Contractor shall continuously identify and correct, with County approval, any single point failures with Mobility Infrastructure Services.

5.11.2.4. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Mobile Infrastructure Services.

5.11.2.5. Contractor shall enable the central management and control all mobile devices (including BYOD), platforms and applications from a single unified console.

5.11.2.6. Contractor shall implement, County approved, device policies for security and data protection using the Mobility Infrastructure Services on all mobile devices (including BYOD).

5.11.2.7. Contractor shall deploy and manage developed or acquired mobile applications within the Mobility Infrastructure Services application store.

5.11.2.8. Contractor shall provide continuous updated documentation that details operation and use Mobility Infrastructure Services and post them on the Service Portal.

5.11.2.9. Contractor shall recommend, for County approval, standards on a yearly basis for all Mobility Infrastructure Services.

5.11.2.10. Contractor shall recommend, for County approval, mobile devices standards including hardware and operating system.

5.11.2.11. Contractor shall facilitate and enable application gateways services for developed or acquired applications, with County approval, to internal County resources from mobile devices using Mobility Infrastructure Services.

5.11.2.12. Contractor shall maintain a continuous timeline/roadmap of all Mobility Infrastructure 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.

5.11.2.13. Contractor shall reference the Standards and Procedures manual for standard Mobile Devices to be supported.

5.11.3. Environment

The following further describe and scope Mobility Infrastructure Services elements supported by Contractor and with which Contractor shall comply.

5.11.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Mobility Infrastructure Services.

5.11.3.2. Technology Refresh

Contractor shall refresh Mobility Infrastructure Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.11.4. Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Mobility Services.

Mobility Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide centralized, secure Mobile Device Management and Support Services for iOS, Android and Windows Phone devices (smartphones or tablets).	X	
2. Perform management and support of mobile devices management application including MDM application updates, configuration and troubleshooting, point releases and fixes as required.	X	
3. Maintain certificates and password resets as required	X	
4. Perform and provide over-the-air (OTA) self-provisioning, policy setting on device and connection configuration, including the ability to set encryption, VPN configuration and Wi-Fi settings with verification to streamline activations and eliminate the need for IT involvement.	X	
5. Provide an Enterprise Mobile Device Application store which can be used for application publishing to devices, through a push by User group (labor for the creation or modification of applications for the Application Store shall be provided through Application Service Requests). The Application Store accessed from all supported devices.	X	
6. Perform and submit operational planning for Mobile Device Management and Support capacity and performance purposes.	X	
7. Review and approve operational planning for Mobile Device Management and Support capacity and performance purposes.		X
8. Design operational views and status reports for the Service Portal.	X	
9. Review and approve operational views and status reports.		X
10. Design operational reports per County request.	X	
11. Review and approve operational reports.		X
12. Produce and submit Mobile Device Management and Support operational policies and procedures including escalation.	X	

Mobility Services Roles and Responsibilities		
13. Review and approve Mobile Device Management and Support operational policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Develop and improve Mobile Device Management and Support build as appropriate to improve performance.	X	
15. Provide all test Services and produce documentation required to support Mobile Device Management and Support Services.	X	
16. Produce and submit all test documentation to County.	X	
17. Review and approve all test documentation.		X
18. Provide all deployment Services required to support Mobile Device Management and Support Services.	X	
19. Produce and submit to County all Mobile Device Management and Support Services deployment documentation.	X	
20. Review and approve all Mobile Device Management and Support Services deployment documentation.		X
21. Produce and submit plans to apply Mobile Device Management and Support Services application releases and patches as required.	X	
22. Review and approve Mobile Device Management and Support Services application releases and patches plans.		X
23. Enforce security to continuously review all connected devices and quarantine or revoke service for unmanaged or compromised devices.	X	
24. Deliver simplification of mobile application deployment with an enterprise-specific over-the-air (OTA) catalog of mandatory, recommended and available applications, without requiring the use of a commercial Application Store such as Google Play or iTunes Store.	X	

Mobility Services Roles and Responsibilities		
25. Provide security management, including the general functionality described in this Resource Unit. The specific settings are defined by County policy as: • Require passcode • Wipe device after too many passcode attempts • Restrict/Permit applications • Restrict/Permit content • Enforce application blacklist/whitelist • Manage device configurations • Manage Exchange and Active sync E-Mail configurations • Provide the ability to manage application sets and tie them to Active Directory • In the event of lost or stolen assets, the asset shall be wiped of all County Data	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Perform routine database maintenance and backups to maintain optimal performance of the Mobile Device Management and Support Services Platform.	X	
27. Maintain the Mobile Device Management and Support Services Platform configuration per engineering build documents and County policy.	X	
28. Maintain all Mobile Device Management and Support Services certificates for the platform and the devices.	X	
29. Perform all device specified Services through the Mobile Device Management and Support Services console (e.g., remote wipes and password resets).	X	
30. Provide continuous monitoring of all connected devices for security Incidents.	X	
31. Quarantine or revoke service for any unmanaged or compromised mobile device.	X	
32. Manage mobile devices through Active Directory group membership.	X	
33. Manage County approved BYOD devices to specific applications authorized by the County.	X	
34. Utilize the Service Portal to monitor system performance.	X	
35. Provide operational reports as requested.	X	

Mobility Services Roles and Responsibilities		
36. Manage Enterprise Application Store to add and delete mobile applications.	X	
37. Provide security protection to maintain control of County information and selectively wipe only County Data and applications, or all data, from managed devices with review of successful completion.	X	
38. Provide County required reporting on Mobile devices usage, billing and invoicing Services.	X	
39. Coordinate between User, Service Desk and Third-Parties such as Mobile/Wireless Carrier or device manufacturer to manage all User and device related Incidents and Service Requests as needed.	X	
40. Provide a single point of contact for the mobile device environment including coordination with Third-Parties as needed.	X	
41. Provide ability to securely access authorized enterprise content from any authorized mobile device.	X	
42. Provide ability to enforce County security and policy through role-based models.	X	
43. Provide for personal and corporate data to securely coexist on the same device.	X	
44. Enable employee self-activation of corporate and personal devices.	X	
45. Provide authorized End-Users access to Service Portal.	X	
46. Provide the ability to monitor device usage and enforce security from a single global console.	X	
47. Provide Services to secure data, applications, communication, and network access from authorized mobile devices.	X	
48. Pre-configure device settings and policies based on ownership models.	X	
49. Provide Services that protect devices from unauthorized use.	X	
50. Provide ability to control specific device features and applications.	X	
51. Provide the ability to enforce authorized Wi-Fi and VPN networks on mobile devices.	X	

Mobility Services Roles and Responsibilities		
52. Provide Services to secure devices, data, applications, communication, and network access.	X	
53. Provide Services that implement secure data leakage prevention.	X	
54. Provide Services that protect against malware and unauthorized access via custom profiles.	X	
55. Support County in performing security and compliance reviews on mobile devices as needed.	X	

5.12. Wireless Network Access Services

5.12.1. Overview

This section pertains to the Wireless Network Access Services Framework Component within the Network Services Framework. The Wireless Network Access Services Framework Component applies to the Wireless Local Area Network (WLAN) located throughout various County Sites. The WLAN allows County End-Users and authorized users to establish a secure connection to the County internal network or an unsecured connection, taken directly to the Internet, for visitors.

Services provided within this Framework Component include, but are not limited to, the following:

- Accessibility to County resources for wireless connected End-Users
- Security from unauthorized users
- Central management of Wireless Network Access Hardware and Software
- Performance better or equal to wired network for secure network access
- Secure network integration
- Network access control
- Network capacity and performance monitoring
- Network engineering
- Transformational activities to improve overall service
- Technical refresh

5.12.2. High Level Requirements

5.12.2.1. Contractor shall maintain technical currency on Wireless Network Access Services Hardware and Software.

5.12.2.2. Contractor shall ensure that all devices attached to the secure network WLAN are valid and authorized.

5.12.2.3. Contractor shall continuously identify and correct, with County approval, any single point failures within the Wireless Network Access Services.

5.12.2.4. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Wireless Network Access Services.

5.12.2.5. Contractor shall deploy WLAN to the secured network for all County authorized, wireless End-Users using appropriate device and user authentication.

5.12.2.6. Contractor shall deploy WLAN to the unsecured network for all County visitors.

5.12.2.7. Contractor shall provide End-User authentication for all interaction with the secure WLAN.

5.12.2.8. Contractor shall deploy device authentication for secure WLAN access using County PKI infrastructure.

5.12.2.9. Contractor shall ensure that the Wireless Network Access Services network is secure by implementing County security policies and using Network Access Control.

5.12.2.10. Contractor shall deploy a guest access portal and splash screen to unsecured WLAN for County visitors.

5.12.2.11. Contractor shall make available two types of Wireless Access Points interior mounted and exterior mounted.

5.12.2.12. Contractor shall continuously maintain a timeline/roadmap of all Wireless Network Access Services Hardware and Software 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.

5.12.3. Environment

The following further describe and scope Wireless Network Access Services elements supported by Contractor and with which Contractor shall comply.

5.12.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Wireless Network Access Services.

5.12.3.2. Technology Refresh

Contractor shall refresh Wireless Network Access Services Wireless Access Points (WAPs) on a 3-year refresh schedule and all other Wireless Network Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.12.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Wireless Network Access Services.

Wireless Network Access Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendation for Wireless Network Access Services architecture.	X	
2. Review and approve Wireless Network Access Services architecture.		X

Wireless Network Access Services Roles and Responsibilities		
3. Produce and submit Wireless Network Access Services refresh plan on a yearly basis.	X	
4. Review and approve Wireless Network Access Services refresh plan on a yearly basis.		X
5. Produce and submit Wireless Network Access Services policies and procedures.	X	
6. Review and approve Wireless Network Access Services policies and procedures.		X
7. Produce and submit Wireless Network Access Services security architecture.	X	
8. Review and approve Wireless Network Access Services security architecture.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Design, test and implement approved Wireless Network Access Services architecture.	X	
10. Deploy, manage, communicate and report on activities related to Wireless Network Access Services refresh.	X	
11. Review and approve Wireless Network Access Services refresh report.		X
12. Develop and implement Wireless Network Access Services policies and procedures.	X	
13. Design, test and implement approved Wireless Network Access Services architecture.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide support, including break-fix, for all Wireless Network Access Services Assets.	X	

5.13. Third-Party Network Access Services

5.13.1. Overview

This section pertains to the Third-Party Network Access Services Framework Component within the Network Services. The Third-Party Network Access Services Framework Component applies to security services, network transport and bandwidth required for Third-Party access to the County network.

Services provided within this Framework Component include, but are not limited to, the following:

- Protection from unauthorized network access
- Firewall services
- Intrusion protection
- Detection and reporting
- Security monitoring
- Data protection
- Network management
- Network capacity and performance monitoring
- Third-Party network to County network connectivity
- User authentication services

5.13.2. High Level Requirements

5.13.2.1. Contractor shall establish and maintain Third-Party Network Access Services to the County secure network.

5.13.2.2. Contractor shall monitor, log and report all activity related to Third-Party Network Access Services.

5.13.2.3. Contractor shall ensure necessary bandwidth and capacity are in place for all Third-Party Network Access Services.

5.13.2.4. Contractor shall ensure all appropriate County security policies are in place and that the County secure network is maintained as safe from compromise.

5.13.2.5. Contractor shall identify and correct, with County approval, any single point failures with Third-Party Network Access Services.

5.13.2.6. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Third-Party Network Access Services.

5.13.3. Environment

The following describes the scope for Third-Party Network Access Services elements supported by Contractor.

5.13.3.1.Hardware and Software

Contractor shall provide all Hardware and Software to support Third-Party Network Access Services.

5.13.3.2.Technology Refresh

Contractor shall refresh Third-Party Network Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.13.3.3.Security Services

Security Services include all the Hardware, Software, and services to ensure secure and authorized access to the County secure network

5.13.3.4.Network Services

Network Services include all the Hardware, Software, and services needed by a Third-Party access to the County secure network. The three (3) categories are private network circuits or connections, Private Circuit/Connection, IPSEC Tunnels and Virtual Access Connections. The circuit connecting to the County is the responsibility of the Third-Party.

5.13.3.4.1. Private Circuit/Connection

- Category 1 — any circuit or connection less than T1 speed (1.544mbps)
- Category 2 — any circuit or connection equal to T1 speed
- Category 3 — any circuit or connection greater than T1 speed

5.13.3.4.2. IPSEC Tunnels Connection

- IPSEC Tunnel 5Mbs
- IPSEC Tunnel 10Mbs

5.13.3.4.3. Virtual Access Connection

- Virtual Access 1Mbps
- Virtual Access 2Mbps
- Virtual Access 3Mbps
- Virtual Access 4Mbps
- Virtual Access 5Mbps
- Virtual Access 5Mbps – Microsoft Teams Rooms (MTR)
- Virtual Access 10Mbps
- Virtual Access 20Mbps
- Virtual Access 30Mbps
- Virtual Access 40Mbps
- Virtual Access 50Mbps

5.13.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Third-Party Network Access Services.

Third-Party Network Access Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Third-Party Network Access Services architecture.	X	
2. Review and approve recommendations for Third-Party Network Access Services architecture.		X
3. Produce and submit plans for monitoring and managing access to the County network from Third-Party entities.	X	
4. Review and approve plans for monitoring and managing access to the County network from Third-Party entities.		X
5. Produce and submit recommendations on firewall policies that comply with County policy.	X	
6. Review and approve firewall policies.		X
7. Produce and submit recommendation of Third-Party Network Access Services Assets refresh or upgrade plan on a yearly basis.	X	
8. Review and approve recommendations on Third-Party Network Access Services Assets refresh or upgrade plan.		X

Third-Party Network Access Services Roles and Responsibilities		
9. Produce and submit plans for Third-Party Network Access Services Asset updates or patches.	X	
10. Review and approve plans for Third-Party Network Access Services Asset updates or patches.		X
Build Roles and Responsibilities	**Contractor**	**County**
11. Design, test and implement approved Third-Party Network Access Services architecture.	X	
12. Design and implement monitoring and managing access plans as approved.	X	
13. Design, test and implement approved firewall policies.	X	
14. Design, test, implement and report Third-Party Network Access Services Assets refresh or upgrade.	X	
15. Review and approve reports for Third-Party Network Access Services Assets refresh or upgrade.		X
16. Design, test and implement updates or patches approved for Third-Party Network Access Services Assets.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
17. Provide support, including break-fix, for all Third-Party Network Access Services Assets.	X	
18. Provide services in conformance to firewall policies and requirements.	X	
19. Support Third-Party Network Access Services refresh.	X	
20. Manage network interfaces between the County and Third-Parties.	X	
21. Produce and submit network utilization, capacity and performance reports.	X	
22. Provide initial review of security Incidents and the determination if escalation, including to County Information Security, is warranted.	X	
23. Provide standardized End-User operations and also custom reports regardless of the End-user's location and/or department.	X	
24. Identify and remove from the network any malicious-code (malware) infected System.	X	

Third-Party Network Access Services Roles and Responsibilities		
25. Identify and provide countermeasures for malware attacks (i.e., both prevention and remediation).	X	
26. Collect all logs and review all Incidents reported by all other security Services (e.g., NIPS, HIPS, penetration testing, and firewall).	X	
27. Maintain log files in accordance with County policies and Service Levels.	X	
28. Provide security reporting.	X	
29. Provide fraud prevention, detection and reporting.	X	

5.14. External DNS Management Services

5.14.1. Overview

This section pertains to the External DNS Management Services Framework Component within the Network Services Framework. The External DNS Management Services Framework Component applies to a cloud-based DNS solution that is available 24/7/365.

Services provided within this Framework Component include, but are not limited to, 24/7/365 DNS availability, improved DNS responsiveness, Web Application Firewall, Geo blocking, Security Monitor, Client Reputation, IP Whitelists / Blacklists, Bot Management, Dynamic Site Accelerator (CDN), defense against DDoS or similar type attacks, distributed Anycast network, primary and secondary DNS services and interface to internal DNS services.

Akamai Fast DNS Service along with Kona Security Service and Bot Management Service are used to provide External DNS Management Services.

5.14.2. High Level Requirements

5.14.2.1. Contractor shall leverage current Akamai Fast DNS Service for External DNS Management Services.

5.14.2.2. Contractor shall support and manage all aspects of External DNS Services including integration to internal DNS services, as needed.

5.14.2.3. Contractor shall maintain DNS to reduce orphan or bad records.

5.14.2.4. Contractor shall continuously identify and correct, with County approval, any single point failures within the External DNS Management Services.

5.14.2.5. Contractor shall facilitate a quarterly meeting with Akamai, Contractor resources and County to review roadmaps, support status and emerging services.

5.14.2.6. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to External DNS Management Services.

5.14.2.7. Contractor shall leverage "Web Application Firewall" component from Kona Security Services to inspect application traffic and block suspicious or known exploits.

5.14.2.8. Contractor shall leverage "Geo Blocking" component from Kona Security Services to block traffic originating from specific geographical locations.

5.14.2.9. Contractor shall leverage "Security Monitor" component from Kona Security Services to provide real-time visibility into network- and application-layer attacks.

5.14.2.10. Contractor shall leverage "Client Reputation" component from Kona Security Services to block attackers proactively when they're detected elsewhere on the Akamai Platform.

5.14.2.11. Contractor shall leverage "IP Whitelists / Blacklists" component from Kona Security Services to define list of IP addresses to allow or block for positive and negative security.

5.14.2.12. Contractor shall leverage "Bot Manager Standard" from Akamai to identify and manage bots targeting the County websites.

5.14.2.13. Contractor shall continuously maintain a timeline/roadmap of all External DNS Management Services Hardware and Software 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.

5.14.3. Environment

The following further describe and scope External DNS Management Services elements supported by Contractor and with which Contractor shall comply.

5.14.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support External DNS Management Services.

5.14.3.2. External Service

Contractor shall own and manage all contracts with cloud based Third-Parties supporting External DNS Management Services.

5.14.3.3. Technology Refresh

Contractor shall refresh External DNS Management Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

Excluded from technology refresh are all cloud based External DNS Management Services. Cloud based Third-Parties update per product release cycles.

5.14.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with External DNS Management Services.

External DNS Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a solution design on External DNS Services.	X	

External DNS Management Services Roles and Responsibilities		
2. Review and approve the solution design for External DNS Services.		X
3. Produce and submit External DNS Services operational procedures.	X	
4. Review and approve External DNS Services operational procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Produce and maintain an authoritative record of externally-visible County services and of internally-visible County services.	X	
6. Produce and maintain an authoritative record of the County's public network address ranges and the physical networks.	X	
7. Develop and submit a continuously emerging architecture to ensure that External DNS Services are highly available during normal operations and that they failover during any unplanned event.	X	
8. Review and approve External DNS documentation and technical architecture.		X
Operate Roles and Responsibilities	**Contractor**	**County**
9. Configure and maintain External DNS Services.	X	
10. Configure and maintain DNS records on external DNS Services provided by Akamai.	X	
11. Maintain domain names for External DNS.	X	
12. Submit any recommended changes to External DNS records for County approval.	X	
13. Review any proposed changes to External DNS records.		X
14. Produce monthly reports showing External DNS records and domains.	X	

5.15. IP Address Management Services

5.15.1. Overview

This section pertains to the IP Address Management Services Framework Component within the Network Services Framework. The IP Address Management Services

Framework Component applies to the single console management of all IPv6 addresses and all IPv4 public and private addresses within the County network.

5.15.2. High Level Requirements

5.15.2.1. Contractor shall allocate IPv4 and IPv6 address ranges within the County.

5.15.2.2. Contractor shall provide Internet routing to all IP address ranges assigned unless otherwise approved by the County Contractor shall provide robust reporting capability that enables detailed tracking of IP address utilization trends.

5.15.2.3. Contractor shall implement and allocate fixed and dynamic IP addresses to the appropriate network-attached device.

5.15.2.4. Contractor shall assign and maintain IP address ranges for all County Locations.

5.15.2.5. Contractor shall provide integrated management of dynamic and static IP address space.

5.15.2.6. Contractor shall provide detection and management of conflicts, overlaps, and duplicates in address space.

5.15.2.7. Contractor shall provide automated discovery of IP address ranges from DHCP scopes.

5.15.2.8. Contractor shall provide continuous synchronization with internal DNS services.

5.15.2.9. Contractor shall provide continuous alignment with Active Directory "Sites and Services" for all in use IP Address ranges.

5.15.2.10. Contractor shall continuously identify and correct, with County approval, any single point failures within the IP Address Management Services.

5.15.2.11. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to IP Address Management Services.

5.15.2.12. Contractor shall continuously maintain a timeline/roadmap of all IP Address Management Services Hardware and Software 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.

5.15.3. Environment

The following further describe and scope IP Address Management Services elements supported by Contractor and with which Contractor shall comply.

5.15.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support IP Address Management Services.

5.15.3.2. Technology Refresh

Contractor shall refresh IP Address Management Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.15.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with IP Address Management Services.

IP Address Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a documentation p allocation of network address ranges for new networks, the assignment of addresses and device names for new servers for DHCP Services.	X	

IP Address Management Services Roles and Responsibilities		
2. Identify an IP Address Management (IPAM) tool that is used for managing and reporting IP address allocations and DHCP configurations.	X	
3. Review and approve an IPAM tool that is used for managing and reporting IP address allocations and DHCP configurations.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Produce and submit IP Address Management design to ensure that DHCP Services are highly available during normal operations and that they failover during any unplanned event.	X	
5. Review and approve IP Address Management design.		X
6. Implement IP Address Management design.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Allocate network address ranges for new networks and assign addresses.	X	
8. Submit any recommended changes to DHCP configuration for County approval.	X	
9. Review and approve any proposed changes to DHCP configuration for approval.		X
10. Configure and maintain IPAM tool.	X	
11. Maintain an accurate record of network numbers and physical networks to which they are assigned.	X	
12. Produce reports showing network range allocations and device name and address assignments as requested by the County.	X	

5.16. New Site Installation Services

5.16.1 Overview

This section pertains to the New Site Installation Services Framework Component within the Network Services Framework. The New Site Installation Services Framework Component applies to the Plan and Build tasks needed for a new, networked County Site.

New Site Installation is composed of two distinct sets of tasks:

1. New Site Install Fixed Component is determined by Site Type. The activities within this component allows the Site to connect to the County network. This Fixed Component is required for the establishment of any New Site and will include, but not limited to:

- Establishing design standards and design for the new Site
- Ordering and coordinate all circuits necessary for the new Site
- Conducting all planning and engineering required to ensure site functionality
- Installing network Hardware and Software
- Provisioning of the New Site

2. New Site Install Variable Component, as set forth in Appendix 1 to Exhibit 16.1-1, is determined by infrastructure of the site and Site Type. Included in the Variable Component are activities that include, but are not limited to:

- Setting up of MDF/IDF
- Installing intra building cable plant including all wall jacks, labels, patch panels, testing and certification of cable plant
- Project management for the installation of these components

The County may choose to contract directly with Third-Party vendors to perform some or all of the New Site Install Variable Component activities.

Site Types are based on the number of Cable Drops that will be installed at the New Site. A Cable Drop is defined as the copper horizontal cable which reaches from the Intermediate Distribution Frame (IDF) to the wall jack. The table below outlines the Cable Drop thresholds for each different Site Types.

Site Type	Minimum Cable Drops	Maximum Cable Drops
I	1,000	or more
II	501	999
III	250	500
IV	50	249
V	11	49
VI	1	10

5.16.2 High Level Requirements

5.16.2.1 Contractor shall establish and maintain a Fixed Component based on Site Type for New Site Installation.

5.16.2.2 Contractor shall establish and maintain Variable Component (e.g. MDF, IDF, backbone cable, etc.) based on Site Type.

5.16.2.35.16.2.3 If the County elects to procure cabling installation services outside the Agreement: 1. Contractor shall receive certification stating that a full test of all Cable Drops have been performed and that the installation meets the provided standards. 2. Contractor shall perform IMARs on the New Site as of the Turnover Date, as defined in the Standards and Procedures Manual. 3. Contractor shall not be held responsible for any defect in workmanship or materials discovered within six months of the Turnover Date. Correction of such defects by the Contractor shall be performed under a Service Request.

5.16.3 Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with New Site Installation Services.

New Site Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Submit Service Request to initiate New Site Installation indicating Site Type.		X
2. Produce and submit plans for New Site Installation including breakdown of variable components.	X	
3. Review and approve plans and scope of work for New Site Installation.		X
4. Produce and submit procedures for New Site Installation.	X	
5. Review and approve procedures for New Site Installation.		X
Build Roles and Responsibilities	**Contractor**	**County**

New Site Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
6. Design and implement New Site Installation.	X	
7. Implement County approved policies and procedures for New Site Installation.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Support New Site Installation policies and procedures.	X	

5.17. Interactive Voice Services

5.17.1. Overview

This section pertains to the Interactive Voice Services (Interactive Voice Response (IVR) within the Network Services Framework. The Interactive Voice Services Framework Component applies to the Hardware and Software needed to operate the service within the County.

Interactive Voice Services shall be defined as an IVR system which provide one or more of the following capabilities:

- Call Recording
- Call Management Reporting
- Speech Recognition Application
- Computer Screen POP
- Wallboard (Physical/Virtual)
- Data Integration (Data Dip)
- Work Force Optimization
- Outbound/Predictive Dialer
- Agent Softphone
- Speech Enabled Customer Surveys

5.17.2. High Level Requirements

5.17.2.1. Contractor shall develop plan, implement and integrate a consolidation, modernization and improvement in overall reliability and failover for all County IVS Services.

5.17.2.2. Contractor shall recommend a plan for County approval, and execute the approved plan for changes to continuously reduce County usage costs for Interactive Voice Services.

5.17.2.3. Contractor shall deploy and maintain Interactive Voice Services to meet service requirements.

5.17.2.4. Contractor shall develop and maintain three (3) categories of IVS: Small, Medium and Large.

5.17.2.5. Contractor shall continuously provide and update documentation that details operation and use of Interactive Voice services and post them on the Service Portal.

5.17.2.6. Contractor shall recommend, for County approval, technology and architectural standards on a yearly basis for all Interactive Voice Services.

5.17.2.7. Contractor shall provide the following changes to Interactive Voice Services systems:

- Additions, changes or deletions to existing call flow/menu prompts
- Additions, changes or deletions to existing routing or transfer points
- Professional voice recording of changes
- Implementation of existing/available/already purchased licenses

5.17.2.8. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Voice Services.

5.17.3. Environment

The following further describes Interactive Voice Services refresh and the three categories to be provided that shall include technical design, licensing, hardware/software maintenance and support and initial user training.

5.17.3.1. Technology Refresh

Contractor shall refresh Interactive Voice Services Hardware and Software on a 5-year refresh schedule unless otherwise agreed by the County in

writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.17.3.2.Small IVS

- 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 RUs

5.17.3.3.Medium IVS

- 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 will provide County contact center agents full functionality whether they are working at their primary County facility, a remote/alternate County site or at home

5.17.3.4.Large IVS

- 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 a constituent call
- 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

5.17.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with IVS Services.

IVS Service Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans for IVS Services.	X	
2. Review and approve plans for IVS Services.		X
3. Produce and submit procedures for IVS Services.	X	
4. Review and approve procedures for IVS Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Design and implement IVS Services.	X	
6. Implement County approved policies and procedures for IVS Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Support IVS Services policies and procedures.	X	

5.18. Mobility Services

5.18.1. Overview

This section pertains to the Mobility Services Framework Component within the Network Services Framework.

Services provided by this Framework Component will include some or all of the following:

- Unlimited voice and data carrier plans
- Standardized mobile devices
- FirstNet mobile network access
- Free calling to Mexico and Canada
- Mobile device tethering
- Mobile WiFi Hotspot

5.18.2. High Level Requirements

5.18.2.1. Contractor shall provide voice, data and text mobile plans.

5.18.2.2. Contractor shall recommend standard mobile devices and hotspot routers for County review and approval using the established EA process.

5.18.2.3. Contractor shall offer for purchase, via the OIC, standard mobile devices and hotspot routers. The specifications of these devices shall be listed in the Standards and Procedures Manual.

5.18.2.4. Contractor shall provide the County with access to the FirstNet nationwide, high-speed, broadband network dedicated to public safety.

5.18.3. Environment

The following further describe, and scope Mobility Services elements supported by Contractor and with which Contractor shall comply.

5.18.3.1. Hardware and Software

Contractor shall provide all, voice and data plans, mobile devices, and mobile hotspots.

5.18.3.2. Technology Upgrade and Refresh

Mobile devices supported within Mobility Services are eligible for replacement or upgrade through purchases from the OIC (leveraging subsidized offers) at the end of its two-year support cycle.

5.18.4. Roles and Responsibilities

Mobility Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide mobile device recommendations and specifications.	X	
2. Review and approve mobile device recommendations and specifications.		X
3. Provide mobile plan features and capabilities.	X	
4. Develop IMAR and Break Fix Helpdesk scripts for Mobility Services.	X	
5. Develop OIC plans for approved mobile device.	X	

Mobility Services Roles and Responsibilities		
6. Provide OIC information for mobile device and RU ordering.	X	
7. Review and approve plans for mobile carrier plans and mobile device processes.		X
Build Roles and Responsibilities	**Contractor**	**County**
8. Build Help Desk Scripts for both mobile devices and carrier plans.	X	
9. Implement Help Desk scripts for mobile carrier and device issues	X	
10. Deploy OIC offerings for mobile devices and carrier plan.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
11. Provision mobile carrier plans as ordered by the County.	X	
12. Ship mobile devices to County end users as ordered thru the OIC.	X	
13. Provide IMAR and Break Fix Helpdesk services for Mobility Services.	X	

6. DATA CENTER SERVICES

6.1. Overview

Data Center Services include the Hardware, Software and services to support County business applications and data in a secure, consolidated, physical Tier 3 or Tier 4 data center. This includes public cloud environments and services if approved by the County. The data center must be capable of providing hybrid services to County approved cloud based applications and services, be a highly virtualized environment with respect to network, storage and servers and must maintain its own installed and secure Internet connection.

Data Center Services Framework consists of the Plan, Build and Operate services that include the Hardware, Software, Locations and services associated with centralized, shared computing environment.

Data Center Services Framework is composed of the following Framework Components:

- Security Services
- Mainframe Services
- Application Infrastructure Services
- Infrastructure Services
- Development and Test Services
- E-Mail Services
- Unified Communications Infrastructure Services
- Storage Services
- Backup and Recovery Services
- Managed Print Services
- Public Key Infrastructure (PKI) Services

6.2. High Level Requirements

6.2.1. Contractor shall recommend, for County approval, qualified Data Center Service Manager as Contractor Key Personnel to manage Data Center Services.

6.2.2. Contractor shall meet the County needs for highly available, reliable, scalable, up-to-date, agile and secure Data Center Services

6.2.3. Contractor shall maintain a stable, reliable infrastructure to support business applications and services throughout the County.

6.2.4. Contractor shall provide a reliable, scalable, responsive, technically current and secure data network within Data Center Services.

6.2.5. Contractor shall provide redundant, secure, Internet connections for County data center operations within the physical data centers.

6.2.6. Contractor shall maintain Data Center Services network so there is not a single point failure thereby assuring County business continues to operate during any unplanned event.

6.2.7. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Data Center Services.

6.2.8. Contractor shall continuously investigate emerging technology and services that improve the overall data center efficiencies, lowers overall data center costs and improves End-User performance and security when interacting with data center services.

6.2.9. Contractor shall continuously incorporate technology security improvements for business requirements without compromising the security, integrity, and performance of the County enterprise and information resources.

6.2.10. Contractor shall continuously refresh and consolidate Data Center Services Hardware and Software to ensure operability supportability and cost optimization.

6.2.11. Contractor shall continuously identify and correct, with County approval, any single point failures found within Data Center Services.

6.2.12. Contractor shall perform centralized management and performance monitoring of Data Center Services.

6.2.13. Contractor shall continuously ensure that all Data Center Services Hardware and Software are operating at optimal and maximum performance.

6.2.14. Contractor shall report performance, capacity results monthly on all Data Center Services.

6.2.15. Contractor shall deliver and review with County on an annual basis all standards, plans, support tools, version changes, infrastructure changes, refresh, or any matter related to the Data Center and used in the Data Center. This may include future efforts by the Contractor to change services within the Data Center that may or may not affect the County.

6.2.16. Contractor shall continuously review, implement and manage software licensing for Data Center Services assuring best value, non-duplicative installs, inventory, consolidated and documented.

6.2.17. Contractor shall maintain a timeline/roadmap of all Data Center 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.

6.2.18. With County approval, Contractor shall provide, integrate, and support public cloud-based environments and services. Specific functional requirements for these services are defined in the relevant Service Framework requirements below based on the solution design for Infrastructure as a Service (Iaas) and/or Platform as a Service (PaaS), e.g., servers, storage, firewalls, databases.

6.3. Environment

6.3.1. Scope of Environment

Data Center Services shall provide Services to all County Locations for all County business functions and external users of County services.

6.3.2. Hardware and Software

Contractor shall provide all Hardware, Software, licenses, tools needed in the delivery of Data Center Services. Contractor shall own, license, provision, install, manage, maintain, and support such Assets.

6.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Data Center Services.

Data Center Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Data Center Services Framework solutions that best meet County business needs.	X	
2. Review and approve recommendations for Data Center Services Framework solutions that best meet County business needs.		X
3. Produce and submit operational planning for Data Center Services Framework capacity and performance purposes.	X	
4. Review and approve operational planning for Data Center Services Framework capacity and performance purposes.		X
5. Produce and submit recommendations for establishing standards, defining architecture and new project initiatives in the Data Center Services Framework.	X	
6. Review and approve recommendations for establishing standards, defining architecture and new project initiatives in the Data Center Services Framework.		X
7. Recommend architectural components and designs to support the approved data center digitization initiatives.	X	
8. Review and approve architectural components and designs to support the approved data center digitization.		X
9. Develop data center architectural transformation roadmaps in support of any digitization activities.	X	
10. Review and approve data center architectural transformation roadmaps in support of any digitization activities.		X
11. Customize technology architecture taxonomy to meet the evolving business needs of the County.	X	
12. Review and approve the technology architecture taxonomy to meet the evolving business needs of the County.		X
13. Produce and submit recommended Data Center Services administration policies and procedures.	X	
14. Review and approve Data Center Services administration policies and procedures.		X

Data Center Services Roles and Responsibilities		
15. Produce and submit operational documentation on system functions, change management, and Incident management processes.	X	
16. Review and approve operational documentation on system functions, change management, and Incident management processes.		X
17. Produce and submit recommendations on hardware standards for Data Center Services Assets.	X	
18. Review and approve hardware standards for Data Center Services Assets.		X
19. Produce and submit recommendation on software standards for Data Center Services Assets.	X	
20. Review and approve software standards for Data Center Services Assets.		X
21. Produce and submit recommendation for upgrades to Data Center Services Assets as needed to meet business needs.	X	
22. Review and approve upgrades to Data Center Services Assets as needed to meet business needs.		X
23. Produce and submit plans for security updates to Data Center Services Assets.	X	
24. Review and approve plans for security updates to Data Center Services Assets.		X
25. Produce and submit yearly Data Center Services asset consolidation strategy.	X	
26. Review and approve yearly Data Center Services asset consolidation strategy.		X
27. Comply with County policies, standards and regulations applicable to County including information systems, personnel, physical and technical security.	X	
28. Develop a single, consolidated data center for production operations.	X	
29. Develop a technology refresh, redundant systems and improved application architecture design.	X	
30. Collaborate with County to provide technology assistance and support with planning and standard setting activities.	X	

Data Center Services Roles and Responsibilities		
31. Develop a secure flexible Services model when and where appropriate so that the County shall have the flexibility to quickly grow or reduce consumption, including (but not limited to): • Mainframe processing • Storage Area Network (SAN) and Network Attached Storage (NAS) • Centralized backups • Centralized monitoring	X	
32. Create all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to County.	X	
Build Roles and Responsibilities	**Contractor**	**County**
33. Provide all design and engineering required to support Data Center Services Framework.	X	
34. Produce and submit to County all design and engineering documentation.	X	
35. Review and approve all design and engineering documentation.		X
36. Provide all test Services required to support Data Center Services Framework.	X	
37. Produce and submit to County all test documentation.	X	
38. Review and approve all test documentation.		X
39. Implement the approved architectural roadmaps and technology architecture taxonomy across the data centers.	X	
40. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices).	X	
41. Deploy code and content using automated tools which include publishing, promoting, and rolling back code and content.	X	
42. Conduct deployment reviews and provide results to County.	X	
43. Review and approve results of deployment reviews.		X
44. Install security patches and security products.	X	
Operate Roles and Responsibilities	**Contractor**	**County**

Data Center Services Roles and Responsibilities		
45. Publish all Data Center Services asset standards on the Service Portal.	X	
46. Provide support, including breakfix, for all Data Center Services Assets.	X	
47. Perform maintenance activities during nonpeak hours (shall be determined in coordination with the County).	X	
48. Provide the County with a system software upgrade list as it becomes available from software suppliers in the form of a technology roadmap that has a timeline based on version life cycle.	X	
49. Measure, monitor, and adjust data center system and network parameters to make certain the required level of performance is maintained.	X	
50. Analyze performance management information of current and expected capacity to make recommendations for server upgrades, load balancing, and functional splitting. Evaluate trend data and factor it into the overall system requirements.	X	
51. Manage event and workload processes across all platforms.	X	
52. Provide technical support for all hardware/equipment of the Data Center computing infrastructure.	X	
53. Support Data Center infrastructure System software (e.g., operating systems, utilities, databases, Middleware).	X	
54. Provide and support Data Center Networks (e.g., LAN, WAN connection) and related operations (e.g., procure, design, build, systems monitoring, Incident diagnostics, troubleshooting, Resolution and escalation, security management, and capacity planning/analysis) as required to meet County computing requirements.	X	
55. Provide and support Data Center-related environmental elements (e.g., HVAC, dual redundant UPS, power, cable plant, fire detection and suppression systems, temperature and humidity controls, and controlled physical access with 24/7/365 manned security).	X	
56. Support applications test-to-production migration activities infrastructure.	X	

Data Center Services Roles and Responsibilities		
57. Implement and coordinate all changes to the Data Center infrastructure including those that affect the Service Levels of any other Framework and Third-Parties.	X	
58. Maintain and provide all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to County.	X	
59. Provide threat scanning services on files uploaded by public to County servers. Monitor and reports threats.	X	

6.5. Security Services

6.5.1. Overview

The Security Services Framework Component of the Data Center Services Framework includes the Hardware, Software, and services needed to maintain overall managed security for the Services. Security Services provided by this Framework Component include, but are not limited to, the following:

- Monitored or managed firewalls or intrusion prevention systems (IPSs)
- Monitored or managed intrusion detection systems (IDSs)
- Monitored or managed multifunction firewalls, or unified threat management (UTM) technology
- Managed or monitored security gateways for messaging or Web traffic
- Security analysis and reporting of events collected from infrastructure logs
- Reporting associated with monitored/managed devices and incident response
- Managed vulnerability scanning of networks, servers, databases or applications
- Distributed denial of service (DDoS) protection
- Monitoring or management of customer-deployed security information and event management (SIEM) technologies
- Monitoring and/or management of advanced threat defense technologies, or the provision of those capabilities as a service
- Transformational activities to improve the overall security, increase performance and lower costs
- Security architecture services

6.5.2. High Level Requirements

6.5.2.1. Contractor shall control physical access to the Data Center.

6.5.2.2. Contractor shall establish secure zones, with County approval, in the Data Center network.

6.5.2.3. Contractor shall lock down all servers (physical or virtual) and storage within the Data Center.

6.5.2.4. Contractor shall scan all applications, prior to release into production, for vulnerabilities.

6.5.2.5. Contractor shall increase visibility into all data communications and data flows between applications within the Data Center and cloud-based applications.

6.5.2.6. Contractor shall ensure necessary throughput for perimeter protection and internal security methods that are fast enough to deeply scan and remediate threats at wire speed.

6.5.2.7. Contractor shall ensure that Data Center architecture is built with a security first mindset.

6.5.2.8. Contractor shall implement a "single pane of glass" approach to management and monitoring Security Services.

6.5.2.9. Contractor shall ensure all Hardware and Software used for the delivery of Security Services is virtual environment aware.

6.5.2.10. Contractor shall provide management, refresh, support, reporting and logging of all firewalls used in the delivery of the Services.

6.5.2.11. Contractor shall provide information event logging, analysis, reporting and management of all Hardware and Software used to provide Security Services.

6.5.2.12. Contractor shall provide log management on cloud-based applications used by the County.

6.5.2.13. Contractor shall provide intrusion detection and prevention systems within the Data Centers.

6.5.2.14. Contractor shall provide unified threat management.

6.5.2.15. Contractor shall update all Hardware and Software used for Security Services to the latest patch, service packs, or other updates promptly to ensure operational integrity.

6.5.2.16. Contractor shall refresh all Hardware and Software used for Security Services on a 4-year cycle unless otherwise approved by the County.

6.5.2.17. Contractor shall ensure that all Hardware and Software used in the delivery of Security Services is identified whether it is leveraged across multiple accounts or dedicated to the County.

6.5.2.18. Contractor shall maintain all Hardware used in the delivery of Security Services to maximize performance with high-speed network operations.

6.5.3. Environment

6.5.3.1. Hardware and Software

Contractor shall provide all Hardware, Software, tools, knowledge databases, logging and analysis and used in the delivery of Security Services. Contractor shall own, provision, install, manage, maintain, and supported such Assets.

6.5.3.2. Facilities

All Data Center based applications, data, services and cloud-based applications managed by the Contractor for Security Services.

6.5.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Security Services.

Security Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a Security architecture for Data Center Services.	X	
2. Review and approve Security architecture for Data Center Services.		X
3. Develop and submit plans for pre-release of Portfolio Applications or any other data center changes scan and vulnerability analysis.	X	
4. Review and approve plan for scan and vulnerability analysis.		X
5. Develop and submit annual operational procedures for data center Security Services.	X	
6. Produce and submit methodology and performance tools to assess and remediate data center security Incidents.	X	
7. Review and approve methodology and performance tools to assess and remediate data center security Incidents.		X
8. Develop and submit design and plans for SIEM tool.	X	
9. Review and approve design and plans for SIEM tool.		X
10. Produce and submit monitoring and managing of all Security Services Hardware and Software.	X	
11. Review and approve monitoring and managing of all Security Services Hardware and Software.		X
12. Produce and submit annual refresh plans for Security Services.	X	
13. Review and approve submit annual refresh plans for Security Services.		
14. Produce and submit security plan for cloud-based services used in hybrid mode.	X	
15. Review and approve security plan for cloud-based services used in hybrid mode.		X
16. Produce and submit lock-down scripts for Data Center Services.	X	

Security Services Roles and Responsibilities		
17. Review and approve lock-down scripts for Data Center Services.		X
18. Develop process to continuously post all documentation developed and maintained in Security Services to the Service Portal.	X	
Build Roles and Responsibilities	**Contractor**	**County**
19. Implement and maintain security architecture in Data Center Services.	X	
20. Develop monthly reports on SIEM and other Incidents affecting security in Data Center Services.	X	
21. Implement single pane management console for Security Services.	X	
22. Perform refresh according to the approved annual refresh plans for Security Services.	X	
23. Implement and monitor security plan for cloud-based services used in hybrid mode.	X	
24. Implement lock-down scripts for Data Center Services.	X	
25. Design, test and implement all policies needed to provide Security Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Review and analyze SIEM activity and report findings monthly.	X	
27. Recommend changes based on operational experiences to the security architecture supporting Security Services.	X	
28. Support all Data Center Services Incidents.	X	
29. Support all Severity 1 Incidents.	X	
30. Continuous review data center for vulnerabilities and recommend corrections promptly.	X	
31. Update Security Services with patches or other updates promptly to assure operational integrity.	X	

6.6. Mainframe Services

6.6.1. Overview

The Mainframe Service Framework Component of Data Center Services applies to the services and support for the Mainframe and AS/400.

6.6.2. High Level Requirements

6.6.2.1. Contractor shall develop, for County approval, and execute plans to retire the Mainframe from the Services.

6.6.2.2. Contractor shall develop, for County approval, and execute plans to retire the A/S400 from the Services.

6.6.2.3. Contractor shall measure Mainframe usage in CPU hours and must correlate CPU hours directly to End-User processing for specific application.

6.6.3. Environment

6.6.3.1. Hardware and Software

6.6.3.1.1. Contractor shall provide all Hardware, Software and utilities to support Mainframe Services.

6.6.3.1.2. All licensing shall be the responsibility of the Contractor for all Hardware and Software used to provide Mainframe Services.

6.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities specific to Mainframe Services.

Mainframe Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans to retire the Mainframe and AS/400 upon Service Request.	X	
2. Review and approve plans to retire the Mainframe and AS/400.		X
3. Produce and submit recommendations for standards on production jobs and Job Control Language (JCL).	X	
4. Review and approve recommendations for standards on production jobs and Job Control Language (JCL).		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Continue to support mainframe and AS/400 operationally.	X	

6.7. Application Infrastructure Services

6.7.1. Overview

This section pertains to the Application Infrastructure Services Framework Component within the Data Center Framework. The Application Infrastructure Services Framework Component applies to all Hardware and Software needed to maintain and support County Portfolio Applications.

The Application infrastructure is a platform of integrated technologies that can manage multiple hosted applications. The Application infrastructure is comprised of application servers, web servers, and database servers and is a core applications architecture component. The Application infrastructure will deliver high performance application services to End-Users, Third-Parties and constituents of the Services. Some of the key functionality of the Application infrastructure includes, but is not limited to, transaction management, clustering, application-to-application messaging, system management, advanced application development tools, proprietary access, and interoperability with legacy technologies. Application infrastructure provides a powerful platform to support and extend a broad range of County Portfolio Applications.

Building a multi-tier architecture is foundational for the Application infrastructure. Example for multi-tier architecture is as follows:

- A first-tier, front-end, browser-based presentation layer
- A middle-tier business logic application or set of applications
- A third-tier, back-end, database and transaction server

Application Infrastructure Services Framework Component include, but are not limited to, Server refresh, operating system update and support, management of server resources, monitor and analyze network performance, overall application performance, server performance and capacity tuning and analysis.

6.7.2. High Level Requirements

6.7.2.1. Contractor shall ensure that County Portfolio Applications are hosted exclusively in the Application Infrastructure Services.

6.7.2.2. Contractor shall provide continuous operating system updates, patches and security hot fixes for Application infrastructure.

6.7.2.3. Contractor shall deploy County preferred and standard virtual servers, virtual storage and virtual network.

6.7.2.4. Contractor shall gain approval by the County for any exception to the virtual first standards.

6.7.2.5. Contractor shall provide annual refresh plans for all virtual services.

6.7.2.6. Contractor shall provide annual server consolidation recommendations.

6.7.2.7. Contractor shall continuously monitor and correct performance Incidents or system degradation for all application servers.

6.7.2.8. Contractor shall maintain Application infrastructure storage on centralized, shared storage environment.

6.7.2.9. Contractor shall provide server hardening across Application infrastructure.

6.7.2.10. Contractor shall implement a data backup strategy to meet County Applications' requirements.

6.7.2.11. Contractor shall support and assist in Third-Party application installation and configuration.

6.7.2.12. Contractor shall improve overall architecture of the Application infrastructure with consideration of cloud and increased virtualization techniques.

6.7.2.13. Contractor shall continuously improve demand levels across the Application infrastructure.

6.7.2.14. Contractor shall continuously improve and reduce costs with integrated tools that provide better security and control of the Application infrastructure.

6.7.2.15. Contractor shall deploy and use standard operating systems on all Hardware used to provide Application Infrastructure Services.

6.7.2.16. Contractor shall continuously improve speed of delivery for new Applications and Services in Application infrastructure.

6.7.2.17. Contractor shall continuously deliver to business objectives while reducing overall Application infrastructure costs across all environments.

6.7.2.18. Contractor shall provide centralized support and tools for Application servers located outside the data center.

6.7.2.19. Contractor shall maintain a timeline/roadmap of all Application Infrastructure 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.

6.7.2.20. Contractor shall maintain and be responsible for all components needed to provide Application Infrastructure Services.

6.7.2.21. Contractor shall maintain Application Infrastructure Services so there is not a single point failure thereby assuring County business applications continue to operate during any unplanned event.

6.7.2.22. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Application Infrastructure Services.

6.7.2.23. Contractor shall continuously investigate emerging technologies and services that improve the overall Application infrastructure

efficiencies, lowers overall costs and improves business application performance and security.

6.7.2.24. Contractor shall provide Low Code Application Platform Services.

6.7.3. Environment

6.7.3.1. Hardware and Software

6.7.3.1.1. Contractor shall provide all Hardware, Software and utilities to support Application Infrastructure Services.

6.7.3.1.2. All licensing shall be the responsibility of the Contractor for all Hardware and Software used to provide Application Infrastructure Services.

6.7.3.2. Wintel Application Infrastructure Services

WINTEL Application Infrastructure Services are the Microsoft Server operating system based virtual and physical servers supporting Application Infrastructure Services.

6.7.3.2.1. Contractor shall recommend, for County approval, annual standards for virtual and physical hardware.

6.7.3.2.2. Contractor shall deploy annual, County approved, virtual and physical hardware standards.

6.7.3.2.3. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.2.4. Contractor shall develop hardware standards shall be set for three classes of physical server types: Small, Medium, Large, and X-Large.

6.7.3.2.5. Contractor shall maintain, with sufficient capacity, a server farm to host all virtual servers.

6.7.3.2.6. Contractor shall develop, install and maintain all storage for Application Infrastructure Services using centralized Storage Area Network (SAN).

6.7.3.2.7. Contractor shall recommend, for County approval, annual standards for Windows Operating Systems for virtual and physical servers.

6.7.3.2.8. Contractor shall maintain operating system currency on all Application Infrastructure Services.

6.7.3.2.9. Contractor shall refresh all physical servers at a rate of 25% per year. No physical server shall be in service longer than 4 years without County written approval.

6.7.3.2.10. Contractor shall perform refresh activities using a straight-line methodology throughout the Contract Year.

6.7.3.2.11. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Application Infrastructure Services.

6.7.3.2.12. Contractor shall responsible for all activities related to virtual or physical server refresh, including business application reinstall and configuration.

6.7.3.3. UNIX Application Infrastructure Services

UNIX Application Infrastructure Services are the UNIX operating system based virtual and physical servers supporting Application Infrastructure Services.

6.7.3.3.1. Contractor shall recommend, for County approval, annual standards for virtual and physical hardware.

6.7.3.3.2. Contractor shall deploy annual, County approved, virtual and physical hardware standards.

6.7.3.3.3. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.3.4. Contractor shall develop hardware standards shall be set for three classes of physical server types: Small, Medium, Large and X-Large.

6.7.3.3.5. Contractor shall develop, deliver, for County approval, and implement an infrastructure to support virtualization of UNIX servers.

6.7.3.3.6. Contractor shall maintain, with sufficient capacity, a server farm to host all UNIX based virtual servers.

6.7.3.3.7. Contractor shall develop, install and maintain all storage for UNIX Application Infrastructure Services using centralized Storage Area Network (SAN).

6.7.3.3.8. Contractor shall recommend, for County approval, annual standards for UNIX Operating Systems for virtual and physical servers.

6.7.3.3.9. Contractor shall maintain, potentially, different sources for UNIX operating systems.

6.7.3.3.10. Contractor shall maintain operating system currency on all UNIX Application Infrastructure Services.

6.7.3.3.11. Contractor shall refresh all physical servers at a rate of 20% per year. No physical server shall be in service longer than 5 years without County written approval.

6.7.3.3.12. Contractor shall perform refresh activities using a straight line methodology throughout the Contract Year.

6.7.3.3.13. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Application Infrastructure Services.

6.7.3.3.14. Contractor shall responsible for all activities related to virtual or physical server refresh, including business application reinstall and configuration.

6.7.3.4. Virtual Application Infrastructure Services

Virtual Application Infrastructure Services are the requirements for supporting Windows Application Infrastructure Services and UNIX Application Infrastructure Services.

A Virtual Guest Server is a logical instance of an operating system and applications environment based on the use of virtualization software on a physical host server (Virtual Host). Virtualization software permits the virtualization of a computing environment to support multiple virtual environments.

6.7.3.4.1. Contractor shall recommend, for County approval, annual standards for Virtual Application Infrastructure to support

Windows Application Infrastructure Services and UNIX Application Infrastructure Services.

6.7.3.4.2. Contractor shall deploy annual, County approved, Virtual Application Infrastructure standards.

6.7.3.4.3. Contractor shall determine the number of virtual guest per virtual host server to ensure maximum efficiency and zero service impact due to performance.

6.7.3.4.4. Contractor shall configure and deploy virtual guests to the same standards, or better to physical servers.

6.7.3.4.5. Contractor shall refresh virtual guest servers based on current operating system standards.

6.7.3.4.6. Contractor shall develop and deliver self-service and policy based infrastructure provisioning to the Virtual Application Infrastructure.

6.7.3.4.7. Contractor shall extend the Virtual Application Infrastructure to include software-defined storage platform (Hyper-Converged Infrastructure) integration as standard methodology.

6.7.3.4.8. Contractor shall extend the Virtual Application Infrastructure to integrate and operate in a heterogeneous or hybrid cloud environments.

6.7.3.4.9. Contractor shall design, deliver (for County approval) and implement software-defined storage that can scale for capacity and performance simultaneous as part of virtual guest provisioning.

6.7.3.4.10. Contractor shall design, deliver and implement high availability, fault tolerance and other similar techniques to minimize or eliminate downtime in the Virtual Application Infrastructure.

6.7.3.4.11. Contractor shall deploy tools to ensure all County Portfolio Applications are virtualized and operating in the Virtual Application Infrastructure as standard practice.

6.7.3.4.12. Contractor shall implement management for the Virtual Application Infrastructure that allows the creation, sharing, deployment and migration of virtual guest servers.

6.7.3.4.13. Contractor shall develop, deliver (for County approval), and implement a centralized content library for virtual templates, virtual appliances, ISO images, and scripts.

6.7.3.4.14. Contractor shall develop and implement cloud management platform for purpose-built hybrid cloud applications.

6.7.3.4.15. Contractor shall develop, deliver (for County approval) and implement capacity and performance tools specifically designed for the Virtual Application Infrastructure environment.

6.7.3.4.16. Contractor shall develop the Virtual Application Infrastructure on Industry standard server virtualization platform.

6.7.3.4.17. Contractor shall build and manage virtualization to optimize infrastructure, automate service delivery and provide high availability to virtual guest servers.

6.7.3.4.18. Contractor shall design, deliver, for County approval and implement the virtual farm required to operate the Application Infrastructure Services.

6.7.3.5. Oracle Exadata Services

6.7.3.5.1. Oracle Exadata Services are the compute and storage system for running Oracle Database software supporting Application Infrastructure Services.

6.7.3.5.2. Contractor shall recommend, for County approval, annual standards for hardware.

6.7.3.5.3. Contractor shall deploy annual, County approved, physical hardware standards.

6.7.3.5.4. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.5.5. Contractor shall develop hardware standards for Eighth Rack server.

6.7.3.5.6. Contractor shall refresh all Oracle Exadata based Application Servers every 5 years. No physical server shall be in service longer than 5 years without County written approval.

6.7.3.5.7. Contractor shall perform refresh activities using a straight-line methodology throughout the Contract Year.

6.7.3.5.8. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Oracle Exadata Services.

6.7.3.5.9. Contractor shall responsible for all activities related to Oracle Exadata based Application servers refresh, including business application reinstall and configuration, except for County-approved remediation of application software.

6.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities specific to Application Infrastructure Services.

Application Infrastructure Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for hardware standards of Application Infrastructure Services Assets on a yearly basis.	X	
2. Review and approve hardware standards for Application Infrastructure Services Assets.		X
3. Produce and submit recommendations for operating system standards for Application Infrastructure Services Assets on a yearly basis.	X	
4. Review and approve operating system standards for Application Infrastructure Services Assets.		X
5. Produce and submit Application Infrastructure Services refresh plan on a yearly basis.	X	
6. Review and approve Application Infrastructure Services refresh plan.		X
7. Produce and submit Application Infrastructure Services storage migration and consolidation plan on a yearly basis.	X	

Application Infrastructure Services Roles and Responsibilities		
8. Review and approve Application Infrastructure Services storage migration and consolidation plan.		X
9. Produce and submit backup/recovery policies and procedures.	X	
10. Review and approve backup/recovery policies and procedures.		X
11. Produce and submit recommendations for Application Infrastructure placement into County Locations.	X	
12. Review and approve recommendations for Application Infrastructure placement into County Locations.		X
13. Produce and submit recommendations for Application Infrastructure Services consolidation plan on a yearly basis.	X	
14. Review and approve Application Infrastructure Services consolidation plan.		X
15. Produce and submit Application Infrastructure Services Assets plans for updates or patches as needed for reliable operations and to maintain security.	X	
16. Review and approve Application Infrastructure Assets Services plans for updates or patches as needed for reliable operations and to maintain security.		X
17. Produce and submit recommendations for monitoring and exceptional conditions procedures.	X	
18. Review and approve monitoring and exceptional conditions procedures.		X
19. Produce and submit recommendations for job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs.	X	
20. Review and approve job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs.		X
21. Recommend replacement or upgrade of County utility software programs with commercially available software to support processing operations.	X	
22. Develop Low Code Application Platform solution design document including but not limited to architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).	X	

Application Infrastructure Services Roles and Responsibilities		
23. Review and approve a Low Code Application Platform solution design document including but not limited to architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).		X
24. Develop standards and governance processes for the Low Code Application environment, including but not limited to release management, code reviews, application specification documentation, and code promotion, under the Low Code Center of Excellence.	X	
25. Review and approve standards and governance processes for the Low Code Application environment, including but not limited to release management, code reviews, application specification documentation, and code promotion, under the Low Code Center of Excellence.		X
Build Roles and Responsibilities	**Contractor**	**County**
26. Provide all design and engineering required to deploy, refresh and support Application Infrastructure Services Assets.	X	
27. Design, test and implement hardware standards for Application Infrastructure Services Assets.	X	
28. Design, test and deploy operating system standards for Application Infrastructure Services Assets.	X	
29. Deploy, manage, communicate and report on activities related to Application Infrastructure Services refresh.	X	
30. Review and approve reports on Application Infrastructure Services refresh.		X
31. Design, test and execute Application Infrastructure Services storage migration and consolidation plan.	X	
32. Implement approved backup/recovery policies and procedures.	X	
33. Design, test and deploy approved Application Infrastructure Services consolidation plans.	X	
34. Test and deploy approved updates or patches to Application Infrastructure Services Assets.	X	
35. Implement the Low Code Application Platform based on the approved solution design document.	X	

Application Infrastructure Services Roles and Responsibilities		
36. Update Low Code Application Platform architecture documents as needed (e.g., enhancements).	X	
37. Review and approve updates to Low Code Application Platform architecture documents.		X
Operate Roles and Responsibilities	**Contractor**	**County**
38. Provide support for Application PreProduction and Application Test Servers.	X	
39. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or breakfix activity.	X	
40. Monitor, operate, maintain and support the Third-Party Applications running on Application servers.	X	
41. Provide automated event monitoring tools that notify Applications Team for immediate response if there is an applicationrelated Incident.	X	
42. Provide support, including breakfix, for all Application Infrastructure Services Assets.	X	
43. Provide support for Application Infrastructure located in County Locations.	X	
44. Provide support for Application Infrastructure Services storage migration and consolidation plan.	X	
45. Perform backups on Application Infrastructure Services Assets as defined.	X	
46. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or breakfix activity.	X	
47. Support send and receive electronic data transmissions (e.g., EDI, FTP).	X	
48. Perform upgrades, updates, and security patching to Application Infrastructure Service Assets.	X	
49. Monitor, operate, maintain and support OS (Operating Systems) installed on Application Infrastructure.	X	
50. Monitor, operate, maintain and support the Third-Party Applications running on Application Infrastructure.	X	
51. Execute standard operating procedures at scheduled times.	X	

Application Infrastructure Services Roles and Responsibilities		
52. Startup and shutdown County online/interactive systems according to defined schedules or upon approved requests.	X	
53. Coordinate and manage Third-Party hardware and software maintenance to meet County requirements.	X	
54. Ensure that System management and monitoring tools do not impact County operations.	X	
55. Provide automated event monitoring tools that shall notify Applications Team for immediate response if there is an applicationrelated problem.	X	

6.8. Infrastructure Services

6.8.1. Overview

This section pertains to the Infrastructure Services Framework Component within the Data Center Framework. Infrastructure Services refers to the agnostic, Hardware, Software, network resources and services required for the existence, operation and management of the County IT and Telecommunications enterprise. Infrastructure Services shall deliver the Services to County End-Users, Third-Parties, and constituents.

The objective is the continuous improvement in the overall availability of Infrastructure Services to meet the requirements of County business needs. This covers the evaluation, design, implementation, measurement and management of Infrastructure Services availability from a component and an end-to-end perspective including new or modified service management methodologies and tools, as well as technology modifications or upgrades to infrastructure systems and components.

Infrastructure Services provided within this Framework Component include, but are not limited to, server/OS management, server refresh, server/OS tuning, storage and backup management, mainframe services, production operations, performance analysis, capacity analysis and monitoring, and Systems management.

Additional Services within this Framework Component include, but are not limited to, DNS, DHCP, End-User Authentication, directory services, software distribution, print services, FTP and file services, certificate services, proxy services, load balancers, application and network acceleration, network services, task/job scheduling, web and

content filtering and any Contractor internal servers/services needed to fully support the delivery of the Services.

6.8.2. High Level Requirements

6.8.2.1. Contractor shall develop, deliver (for County approval), and implement on an annual basis currency of software across all Infrastructure Services.

6.8.2.2. Contractor shall determine critical business impact to component or system failures in Infrastructure Services.

6.8.2.3. Contractor shall continuously analyze, identify and remediate single point failures in Infrastructure Services.

6.8.2.4. Contractor shall design, deploy and maintain software distribution for Desktop Computing Services and shall integrate and perform software delivery for County mobile devices.

6.8.2.5. Contractor shall continuously monitor and perform maintenance on all load balancers to ensure optimal operational performance.

6.8.2.6. Contractor shall recommend, for County approval, annual standards for Infrastructure Services.

6.8.2.7. Contractor shall deploy and support current standards within Infrastructure Services.

6.8.2.8. Contractor shall provide centralized and standardized system that automates network management of End-User data, security, and distributed resources.

6.8.2.9. Contractor shall automate software distribution including delivering applications, images, and patches to the environment using industry standard tools.

6.8.2.10. Contractor shall perform comprehensive infrastructure testing for all components in an integrated environment for compute, storage, network, database in a physical or virtual environment.

6.8.2.11. Contractor shall ensure County Public Library private network is included in all Infrastructure Services.

6.8.2.12. Contractor shall provide refresh on all Infrastructure Services Hardware and Software on a four (4) year refresh cycle.

6.8.2.13. Contractor shall ensure the Infrastructure Services storage is not comingled with County End-User or Portfolio Application storage.

6.8.2.14. Contractor shall develop Infrastructure Services to include provisions for hybrid-computing and ensure the complete integration of all County cloud based services.

6.8.2.15. Contractor shall ensure that Infrastructure Services are not comingled with County Applications Infrastructure Services.

6.8.2.16. Contractor shall continuously perform capacity planning, utilization analysis for all Infrastructure Services, including the virtual environments.

6.8.2.17. Contractor shall manage and certify OS images used to support Infrastructure Services.

6.8.2.18. Contractor shall ensure Infrastructure Services must be designed and maintained to support County business strategy and County Portfolio Applications.

6.8.2.19. Contractor shall continuously monitor, report and remediate performance Incidents with Infrastructure Services.

6.8.2.20. Contractor shall ensure end-to-end infrastructure, to include mobile, for all County End-User interaction with the Services.

6.8.2.21. Contractor shall ensure Infrastructure Services includes data centers, Locations, colocation facilities, or hosting/cloud services.

6.8.2.22. Contractor shall deploy and maintain application and network acceleration in the delivery of the Services.

6.8.2.23. Contractor shall continuously improve Infrastructure Services performance, speed and decrease overall latency in the delivery of the Services.

6.8.2.24. Contractor shall continuously deliver to meet County business objectives while reducing overall Infrastructure Services costs.

6.8.2.25. Contractor shall provide centralized support and tools for Infrastructure Services located with the data center or outside the data center.

6.8.2.26. Contractor shall maintain a timeline/roadmap of all Infrastructure 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.

6.8.2.27. Contractor shall maintain and be responsible for all components needed to provide Infrastructure Services (e.g. load balancers, firewalls, IPS).

6.8.2.28. Contractor shall maintain Infrastructure Services so there is not a single point failure thereby assuring County business applications continue to operate during any unplanned event or outage.

6.8.2.29. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Infrastructure Services.

6.8.2.30. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.8.2.31. County may request, on a Service Request, network and application acceleration for a specific County site.

6.8.3. Environment

6.8.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Infrastructure Services.

6.8.3.2. Facilities

Infrastructure Services Hardware or Software placed in County Locations, with County approval, in order to meet the Service Levels and maintain operational efficiencies.

6.8.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Infrastructure Services.

Infrastructure Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for improvement to Infrastructure Services.	X	
2. Review and approve improvement to Infrastructure Services.		X
3. Produce and submit recommendations for Infrastructure Server placement into Locations.	X	
4. Review and approve recommendations for Infrastructure Server placement into Locations.		X
5. Produce and submit recommendations for hardware standards of Infrastructure Server Services Assets on a yearly basis.	X	
6. Review and approve hardware standards for Infrastructure Server Services Assets.		X

Infrastructure Services Roles and Responsibilities		
7. Produce and submit recommendations for operating system standards for Infrastructure Server Services Assets on a yearly basis.	X	
8. Review and approve operating system standards for Infrastructure Server Services Assets.		X
9. Produce and submit Infrastructure Server Services refresh plan on a yearly basis.	X	
10. Review and approve Infrastructure Server Services refresh plan.		X
11. Produce and submit recommendations for Infrastructure Server Services consolidation plan on a yearly basis.	X	
12. Review and approve Infrastructure Server Services consolidation plan.		X
13. Produce and submit Infrastructure Server Services Assets plans for updates or patches as needed for reliable operations and to maintain security.	X	
14. Review and approve Infrastructure Server Services Assets plans for updates or patches as needed for reliable operations and to maintain security.		X
Build Roles and Responsibilities	**Contractor**	**County**
15. Provide all design and engineering required to deploy, refresh and support Infrastructure Server Services Assets.	X	
16. Design, test and implement approved improvements to Infrastructure Services.	X	
17. Design, test and implement hardware standards for Infrastructure Server Services Assets.	X	
18. Design, test and deploy operating system standards for Infrastructure Server Services Assets.	X	
19. Deploy, manage, communicate and report on activities related to Infrastructure Server Services refresh.	X	
20. Review and approve reports on Infrastructure Server Services refresh.		X
21. Design, test and deploy approved Infrastructure Server Services consolidation plans.	X	
22. Test and deploy approved updates or patches to Infrastructure Server Services Assets.	X	

Infrastructure Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
23. Manage Infrastructure Server Services to meet performance Service Levels.	X	
24. Maintain and support the Public Library public infrastructure web filtering.	X	
25. Manage bandwidth and latency constraints and minimize impacts during automated software deployment.	X	
26. Provide deployment Services using automated tools for remote access/VPN Users.	X	
27. Provide deployment reports to include success and failure statistics of scheduled distributions — such as patches or upgrades.	X	
28. Provide support, including break-fix, for all Infrastructure Server Services Assets.	X	
29. Provide support for Infrastructure Servers located in Locations.	X	
30. Conduct data and Infrastructure migration that is necessary due to any Infrastructure Server Services refresh or break-fix activity.	X	
31. Perform upgrades to Infrastructure Server Services Assets.	X	
32. Monitor, operate, maintain and support OS (Operating Systems) installed on Infrastructure Server Services Assets.	X	
33. Manage Infrastructure Server Services to meet performance Service Levels.	X	
34. Maintain and support the Public Library public infrastructure web filtering.	X	
35. Manage bandwidth and latency constraints and minimize impacts during automated software deployment.	X	
36. Provide deployment services using automated tools for remote access/VPN users.	X	
37. Provide deployment reports to include success and failure statistics of scheduled distributions — such as patches or upgrades.	X	

6.9. Development and Test Services

6.9.1. Overview

This section pertains to the Development and Test Services Framework Component within the Data Center Framework. Development and Test Services are the activities associated with ensuring that all individual technical components configured with or added to the Services work together cohesively to achieve the intended results prior to release to the Production environment.

The activities associated with these Services delivered virtually.

6.9.2. High Level Requirements

6.9.2.1. Contractor shall develop, deliver, for County approval, and implement a private cloud based/hybrid Development and Test Services.

6.9.2.2. Contractor shall build and maintain the Development and Test Services Infrastructure to all standards and in close alignment with the production environment.

6.9.2.3. Contractor shall support in-flight projects, planned projects, maintenance projects and new application releases.

6.9.2.4. Contractor shall manage existing test environments, build new test environments and provide additional capacity on demand via the cloud or other approved County solution.

6.9.2.5. Contractor shall establish the processes and controls that are required to place a County Portfolio Application Development and Test environment in the cloud.

6.9.2.6. Contractor shall develop automation in the management, provision and support of the Development and Test Services Infrastructure to maximize overall system efficiencies.

6.9.2.7. Contractor shall ensure Development and Test Services Infrastructure is integrated into Run Book automation.

6.9.2.8. Contractor shall develop, deliver and maintain cloud orchestration for Development and Test Services Infrastructure.

6.9.2.9. Contractor shall continuously improve overall test environment builds to achieve high efficiencies and accurate test environments.

6.9.2.10. Contractor shall develop the Development and Test Services Infrastructure with a high level of reuse and maximize investments in current tools and technology.

6.9.2.11. Contractor shall continuously develop and implement improvements to overall availability of the Development and Test Services Infrastructure.

6.9.2.12. Contractor shall develop, deliver and implement proper scheduling techniques to maximize the use of the Development and Test Services Infrastructure.

6.9.2.13. Contractor shall develop, deliver and implement processes to ensure the Development and Test Services Infrastructure is not underutilized.

6.9.2.14. Contractor shall ensure sufficient capacity in the Development and Test Services Infrastructure to meet County demand.

6.9.2.15. Contractor shall develop an on-demand Development and Test Services Infrastructure that scales up or down to meet demand.

6.9.2.16. Contractor shall develop, deliver and implement process to cold store virtual and unused workload not currently needed in the Development and Test Services Infrastructure.

6.9.2.17. Contractor shall develop, deliver, for County approval, and implement a fully virtual Development and Test Services Infrastructure.

6.9.2.18. Contractor shall not use any physical servers for the Development and Test Services Infrastructure, without prior County approval.

6.9.2.19. Contractor shall develop, deliver and maintain interfaces to production environment as needed to meet business needs.

6.9.2.20. Contractor shall implement and integrate Identity Access Management Services in the Development and Test Services Infrastructure.

6.9.2.21. Contractor shall replicate production security architecture, to the extent possible, in the Development and Test Services Infrastructure.

6.9.2.22. Contractor shall ensure Development and Test Services Infrastructure duplicates production to the extent possible.

6.9.3. Environment

6.9.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Development and Test Services Infrastructure Services.

6.9.3.2. Licenses

Contractor shall provide all licenses for all cloud based Development and Test Services.

6.9.4. Roles and Responsibilities

The following table identifies the Development and Test Services roles and responsibilities that Contractor and County shall perform.

Development and Test Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop and submit design for Development and Test Services.	X	
2. Review and approve design for Development and Test Services.		X
3. Develop and submit procedures for managing Development and Test environment to closely align with production.	X	
4. Review and approve procedures for managing Development and Test environment.		X

Development and Test Services Roles and Responsibilities		
5. Develop and submit management plan for capacity and moving workloads on and off.	X	
6. Review and approve management plan.		X
7. Develop and submit plans and design for hybrid cloud integration for Development and Test Services.	X	
8. Review and approve plans and design for hybrid cloud integration for Development and Test Services.		X
9. Design and submit a Development and Test Environment that is all virtual.	X	
10. Review and approve all virtual design.		X
Build Roles and Responsibilities	**Contractor**	**County**
11. Implement design for Development and Test Services.	X	
12. Implement procedures for managing Development and Test environment to closely align with production.	X	
13. Implement management plan for capacity and moving workloads on and off.	X	
14. Implement automated provisioning tools.	X	
15. Implement security architecture, as closely as possible, in the Development and Test environment.	X	
16. Implement full Identity Management Access for Development and Test Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
17. Manage all break-fix and Incidents in the Development and Test environment.	X	
18. Manage all workloads in the Development and Test environment for only work in progress is hosted	X	
19. Manage cold storage of virtual images not currently in use.	X	
20. Manage and support process to copy current production environment applications into the Development and Test Environment.	X	
21. Manage and provide all updates to Runbooks and other documentation for Portfolio Applications.	X	

Development and Test Services Roles and Responsibilities		
22. Manage all licenses needs to fully operate the Development and Test Environment.	X	
23. Manage the Development and Test Environment to ensure all work can be accomplished on schedule.	X	
24. Develop, manage and post the schedule for all work to be performed in the Development and Test Environment.	X	
25. Produce monthly reports on usage in the Development and Test Environment.	X	
26. Produce monthly reports on images and applications active and in cold storage in the Development and Test Environment.	X	

6.10. E-Mail Services

6.10.1. Overview

This section pertains to the Electronic Mail (E-Mail) Services Framework Component within the Data Center Framework. E-Mail is a critical service used by all County End-Users as a daily business, must-have productivity tool. E-Mail Services must ensure the safe and reliable uninterrupted delivery of E-Mail to County End-Users and external entities.

The E-Mail Services Framework Component applies to all Hardware, Software, services and policies needed to maintain and support E-Mail Services.

6.10.2. High Level Requirements

6.10.2.1. Contractor shall develop, for County approval, plans to migrate and upgrade E-Mail Services during Transition.

6.10.2.2. Contractor shall design, and deliver, for County approval, and implement a highly reliable, high redundant E-Mail Services platform that ensures zero data loss.

6.10.2.3. Contractor shall provide perimeter services that protect against SPAM and E-Mail Worms or malicious software of any sort.

6.10.2.4. Contractor shall design, deliver (for County approval) and implement secure E-Mail remote access (e.g. Outlook Web Access).

6.10.2.5. Contractor shall implement Microsoft Exchange for E-Mail Services.

6.10.2.6. Contractor shall maintain and upgrade Microsoft Exchange software versions within 12 months of major releases and within 3 months for minor releases.

6.10.2.7. 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.

6.10.2.8. Contractor shall recommend a plan for County approval, and execute the approved plan for e-discovery services authorized by a Service Request.

6.10.2.9. Contractor shall integrate fax capabilities into E-Mail Services for End-Users.

6.10.2.10. Contractor shall recommend a plan for County approval, and execute the approved plan for DLP protection per County policies for E-Mail Services.

6.10.2.11. Contractor shall ensure and continuously update for each mailbox protection against any anti-malware and anti-spam or any other malicious product or vulnerability.

6.10.2.12. Contractor shall ensure that secure mobile access to E-Mail Services is provided to County-furnished or approved BYOD mobile devices.

6.10.2.13. Contractor shall apply County retention policy across all mailboxes without exception.

6.10.2.14. Contractor shall apply and provide unlimited mailbox storage for each mailbox.

6.10.2.15. Contractor shall recommend a plan for County approval, and execute the approved plan for in-place archiving on all mailboxes as an alternate storage location for historical messaging data (eliminate PST).

6.10.2.16. Contractor shall provide in-place hold to selected mailboxes, via Service Request, to preserve all mailbox items immutably for a specified period of time.

6.10.2.17. Contractor shall recommend a plan for County approval, and execute the approved plan for integrated digital signing to all mailboxes leveraging County PKI platform.

6.10.2.18. 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.

6.10.2.19. Contractor shall ensure through continuous review and report that all End-User mailboxes comply with the County's E-Mail retention policy.

6.10.2.20. Contractor shall recommend a plan for County approval, and execute the approved plan for a more secure OWA solution that protects County Data and maintains simplified End-User interaction and authentication.

6.10.2.21. 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.

6.10.2.22. 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.

6.10.2.23. Contractor shall enable End-Users an expiration date for sent encrypted E-Mail messages.

6.10.2.24. Contractor shall provide self-help password administration for recipients of encrypted E-Mails that permit passwords to be established and reset.

6.10.2.25. Contractor shall ensure high delivery of cloud based E-Mail Services and complete End-User integration.

6.10.2.26. Contractor shall provide centralized support and tools for E-Mail Services hosted within the data center or hosted outside the data center.

6.10.2.27. 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.

6.10.2.28. Contractor shall maintain and be responsible for all components needed to provide E-Mail Services (e.g. load balancers, firewalls, IPS).

6.10.2.29. 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.

6.10.2.30. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to E-Mail Services.

6.10.2.31. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.10.2.32. Contractor shall provide a Virtual Fax solution, which offers inbound fax capabilities to a group O365 mailbox, together with outbound fax capabilities from a group O365 mailbox.

6.10.2.33. Contractor shall also provide set up and porting services, when porting the analog number is possible, together with maintenance and break/fix.

6.10.3. Environment

6.10.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support E-Mail Services

6.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with E-Mail Services.

E-Mail Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit E-Mail Services operational and computing procedures.	X	
2. Review and approve E-Mail Services operational and computing procedures.		X
3. Produce and submit E-Mail Services architecture.	X	
4. Review and approve E-Mail Services architecture.		X
5. Produce and submit recommendations for E-Mail application standards on a yearly basis.	X	
6. Review and approve E-Mail application standards.		X
7. Produce and submit backup/recovery policies and procedures.	X	
8. Review and approve backup/recovery policies and procedures.		X
9. Produce and submit defining policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.	X	

E-Mail Services Roles and Responsibilities		
10. Review and approve policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.		X
11. Produce and submit plans to update and patch E-Mail Services to maintain reliability and security.	X	
12. Review and approve plans to update and patch E-Mail Services to maintain reliability and security.		X
13. Produce and submit procedures for directory synchronization with County departments.	X	
14. Review and approve procedures for directory synchronization with County departments.		X
15. Produce and submit plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.	X	
16. Review and approve plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.		X
17. Produce and submit End-User tip sheets on use of E-Mail Services.	X	
18. Develop procedures for E-Mail.	X	
19. Review and approve plans and procedures to allow County End-Users to encrypt E-Mails to external addresses.		X
20. Produce and submit End-User tip sheets on use of E-Mail Services including encryption.	X	
21. Review and approve for distribution End-User tip sheets on use of E-Mail Services.		X
22. Produce and submit plans for E-Mail integrated Fax solution.	X	
23. Review and approve E-Mail integrated Fax solution.		X
Build Roles and Responsibilities	**Contractor**	**County**
24. Design and implement E-Mail Services operational and computing procedures.	X	
25. Design, test and implement approved changes to the E-Mail application.	X	
26. Design, test and deploy E-Mail server refresh according to the approved plan.	X	

E-Mail Services Roles and Responsibilities		
27. Design and implement policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.	X	
28. Design, test and implement approved updates and patches to E-Mail Services.	X	
29. Design, test and implement directory synchronization with out-of-scope County departments.	X	
30. Design, test and implement approved plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.	X	
31. Design, test and implement approved plans and procedures used by Data Center in order to allow County End-Users to encrypt E-Mail being sent to external addresses.	X	
32. Provide encryption plug-ins for Outlook clients.	X	
33. Deploy and install encryption profiles to E-Mail encryption End-Users.	X	
34. Implement approved backup/recovery policies and procedures.	X	
35. Distribute End-User approved tip sheets.	X	
36. Implement E-Mail retention policies.	X	
37. Design and implement E-Mail integrated Fax solution.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
38. Provide support, including break-fix, for all E-Mail Services Assets.	X	
39. Manage and support E-Mail Services to meet operational and computing procedures.	X	
40. Manage and support the E-Mail application.	X	
41. Support and provide E-Mail accounts to End-Users.	X	
42. Provide and support migration of End-User mailboxes in support of E-Mail server refresh or break-fix activity.	X	
43. Manage and support directory synchronization operations.	X	
44. Manage and support SPAM Services and other specific Services needed to protect End-Users.	X	

E-Mail Services Roles and Responsibilities		
45. Manage and maintain E-Mail accounts and E-Mail SMTP addresses.	X	
46. Manage and maintain E-Mail URL filtering Services to protect End-Users.	X	
47. Manage and support E-Mail encryption Services.	X	
48. Manage and maintain E-Mail Services to Service Levels.	X	
49. Perform backups on E-Mail Services Servers Assets as defined.	X	
50. Support E-Mail retention policies per County policy.	X	
51. Manage and support integrated Fax Services.	X	
52. Produce encryption resource unit reports monthly.	X	
53. Manage and Maintain E-Mail encryption accounts for End-Users.	X	

6.11. Unified Communications Infrastructure Services

6.11.1. Overview

This section pertains to the Unified Communications Infrastructure Services Framework Component within the Data Center Services Framework. The Unified Communications Infrastructure Services offering includes all the Framework Components needed to ensure enhanced, mobile, flexible, and more collaborative working environment through a single unified experience for County End-Users.

These Services include:

- Software deployment/management Services
- Management of distribution lists (DLs) and Unified Communication Integration Services (for example, presence management for User availability, voice/IM communications across multiple End-User devices, etc.)
- Acquisition, installation, upgrades, maintenance, support and tuning of collaborative computing Services (e.g., MS Exchange, Audio/Video and Web Conferencing etc.)
- Dedicated Real-Time Collaboration Services
- Synchronous Text Exchange
- Presence Awareness

- Peer-to-Peer Collaboration
- Audio/Video
- MS Lync
- Web Conferencing (Live Meeting)
- Mobile Support
- Utilization Reporting
- Federated Services shall be provided to external agencies approved by the County

The County currently uses Microsoft Office 365 Skype for Busines to provide Unified Communications Infrastructure Services

6.11.2. High Level Requirements

6.11.2.1. Contractor shall provide End-Users the ability to exchange text messages in real time (chat).

6.11.2.2. Contractor shall ensure the logging of any activity in Unified Communications Infrastructure Services shall be administratively disabled.

6.11.2.3. Contractor shall provide End-Users with presence capability.

6.11.2.4. Contractor shall provide End-User with the ability to share text, files, whiteboards and presentations.

6.11.2.5. Contractor shall provide all Unified Communications Infrastructure Services to County mobile devices.

6.11.2.6. Contractor shall provide scheduling of live meetings, web conferences, presentations for internal End-Users and external entities.

6.11.2.7. Contractor shall provide monthly utilization reports of all activity posted on the Service Portal.

6.11.2.8. Contractor shall integrate Unified Communication Infrastructure Services with Identity Access Management Services for all End-User authentication.

6.11.2.9. Contractor shall federate, per Service Request, any external entity into Unified Communication Infrastructure Services.

6.11.2.10. Contractor shall maintain and upgrade Unified Communication Infrastructure Services software versions within 12 months of major releases and within 3 months for minor releases.

6.11.2.11. Contractor shall provide integration for all Unified Communication Infrastructure Services with the E-Mail Services distribution lists.

6.11.2.12. Contractor shall maintain a timeline/roadmap of all Unified Communication Infrastructure 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.

6.11.2.13. Contractor shall maintain and be responsible for all components needed to provide Unified Communication Infrastructure Services (e.g. load balancers, firewalls, IPS).

6.11.2.14. Contractor shall maintain Unified Communication Infrastructure Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.

6.11.2.15. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Unified Communication Infrastructure Services.

6.11.2.16. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.11.3. Environment

6.11.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Infrastructure Services

6.11.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Unified Communication Infrastructure Services.

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop Unified Communications Infrastructure Services administration policies (including standards and procedures (new and/or updates) and review with the County.	X	
2. Produce and submit Unified Communications Infrastructure Services architecture.	X	
3. Review and approve Unified Communications Infrastructure Services architecture.		X
4. Review and approve/modify recommended/updated policies, standards and procedures.		X
5. Develop and document final operating procedures for all Unified Communications Infrastructure Services that meet the County requirements and adhere to defined policies and standards.	X	
6. Review and approve/modify final operating procedures documentation.		X
7. Define and submit collaborative computing services procedures.	X	
8. Review and approve collaborative computing services procedures.		X

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
9. Provide the County a briefing on upcoming trends in Unified Communications solutions on a regular basis.	X	
10. Identify process improvements to the Unified Communications service management function.	X	
11. Develop a failover plan for Unified Communications Infrastructure Services.	X	
12. Review and approve/authorize improvement recommendations		X
Build Roles and Responsibilities	**Contractor**	**County**
13. Procure and provision Unified Communications Infrastructure Services.	X	
14. Work with appropriate service delivery personnel to perform the installation, testing, and tuning of all technical environment hardware, software, peripherals and interfaces related to supporting Unified Communications Infrastructure Services platform.	X	
15. Deploy and manage Unified Communications Infrastructure Services, including post-deployment support and warranties.	X	
16. Perform end-to-end Incident determination and resolution for all Unified Communications Infrastructure Services related Incidents.	X	
17. Provide and support Remote Access Services for Unified Communications Infrastructure Services.	X	
18. Ensure that all activities affecting the Unified Communications Infrastructure Services environment(s) are coordinated and communicated through defined change management/change control processes and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
19. Support and participate in any upgrades or migrations and provide applicable services to upgrade infrastructure relating to Unified Communications Infrastructure Services platform.	X	
20. Manage, implement and coordinate all changes to the Unified Communications Infrastructure Services infrastructure.	X	

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
21. Create, maintain and provide all appropriate project plans, project time, technical specifications, management documentation and management reporting in a format that is acceptable to the County.	X	
22. Define monitoring requirements for Unified Communications Infrastructure Services.	X	
23. Develop and document monitoring procedures that meet requirements.	X	
24. Review and approve monitoring procedures.		X
25. Provide proactive and scheduled console monitoring of Unified Communications Infrastructure Services infrastructure and systems (e.g., Servers, Network and backups), respond to messages and take corrective action as required.	X	
26. Coordinate with technical support, Incident & Problem Management and Third-Parties in Incident & Problem resolution.	X	
27. Prepare reports on Unified Communications Infrastructure Services performance and review with the County.	X	
28. Administer the day-to-day interfacing with Third-Parties authorized by the County.	X	
29. Provide troubleshooting, repair and escalation of Incidents in the Unified Communications Infrastructure Services platform environment.	X	
30. Verify the integrity of all messaging backups/monthly restore tests.	X	
31. Ensure stability of the current environment is maintained during deployment of minor upgrades and software release maintenance, emergency software and/or hardware fixes/patches.	X	
32. Provide and utilize scheduling tools and processes for managing mailbox moves, archiving, and Unified Communications Infrastructure Services administration.	X	
33. Review and approve retention/backup/recovery requirements.		X

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
34. Evaluate, coordinate and install patches as required to all Unified Communications Infrastructure Services (e.g., Hotfixes).	X	
35. Install service pack releases, as applicable.	X	
36. Check messaging logs, server logs and event monitoring.	X	
37. Provide and support Instant Messaging (IM) that utilize the Messaging system infrastructure and include a "Presence" status, application sharing, desktop sharing, and remote access functionalities.	x	
38. Provide technical assistance and subject matter expertise support as required by the County staff and Third-Party solution suppliers.	X	
39. Deploy software and systems that provide Unified Communications Infrastructure Services Services.	X	
40. Maintain (e.g., update to new releases, apply patches and fixes, etc.) Unified Communications Infrastructure Services software and systems. Perform activities or coordinate with appropriate parties.	X	
41. Perform break-fix support activities as required, remotely or on-site as needed.	X	

6.12. Storage Services

6.12.1. Overview

This section pertains to the Storage Services Framework Component within the Data Center Services Framework.

Storage Services is a Third-Party agnostic set of storage infrastructure based on the following three primary categories:

- Attached Storage – applies to direct attached storage, considered non-standard, used to meet Service Levels or to meet performance expectations
- SAN Storage - applies to a standard, centralized and consolidated storage environment

- Immutable Storage - applies to dedicated storage environment for maintaining a legal copy of records that are not modifiable or changeable

Storage Services includes, but are not limited to, End-User access, recovery (via backup and replication) of all Storage Services, data protection, storage availability, storage performance, storage reporting to the Business Group, low org or End-User, storage capacity analysis, and storage management. In addition, Storage Services includes, but are not limited to, storage consolidation, tiered storage, performance monitoring, archiving and replication.

Listed below are the specific tiers of storage definitions:

- Primary Tier –High Performance SAN used for Application Infrastructure Services
- Secondary Tier – Lower performing tier used for End-User data, replicated data (applications) and Infrastructure Services
- Archive Tier – archive storage based on age and inactivity Shared Storage Environment using low cost network storage devices .as approved by the County
- Immutable Tier –Immutable Storage using the replicated immutable storage devices as approved by the County
- Attached – direct connect storage
- Document Processing Center 1 – consists of two dedicated storage systems with 17TB Tier 1 Storage and 23 Tier 2 Storage, to support high throughput, imaging applications and will be located at a County Site
- Document Processing Center 2 – consist of two dedicated storage systems with 8TB Tier 1 Storage and 11 Tier 2 Storage, to support high throughput, imaging applications and will be located at a County Site

6.12.2. High Level Requirements

6.12.2.1. Contractor shall deliver dedicate Immutable Tier to the County.

6.12.2.2. Contractor shall develop plans, for County approval, and implement migration any attached storage used in the Application Infrastructure Services to SAN Storage.

6.12.2.3. Contractor shall support, manage and refresh DPC storage located at specific County Sites.

6.12.2.4. Contractor shall ensure all Application Infrastructure Services are integrated into SAN Storage.

6.12.2.5. Contractor shall develop and maintain a centralized, integrated, Storage Service solution for all County Data.

6.12.2.6. Contractor shall eliminate storage underutilization and avoid "islands of storage".

6.12.2.7. Contractor shall continuously decrease overall recovery times in Storage Services.

6.12.2.8. Contractor shall perform centralized management for Storage Services and in storage administration.

6.12.2.9. Contractor shall design, deliver, for County approval and implement separate storage environments for County Data and backup, replicated or mirrored data.

6.12.2.10. Contractor shall deliver dedicated, for County use only, Immutable Storage as part of the Storage Services.

6.12.2.11. Contractor shall measure and report Storage Services by installed, usable capacity.

6.12.2.12. Contractor shall not include any replicated, backup or DR data in the measurement of installed and usable capacity.

6.12.2.13. Contractor shall retain responsibility for storage related to backup and recovery.

6.12.2.14. Contractor shall maintain replication of Immutable Storage.

6.12.2.15. Contractor shall develop, deliver, for County approval, and implement processes to manage and control data growth across Storage Services.

6.12.2.16. Contractor shall develop, deliver, for County approval, and implement processes and controls for the elimination of unmanaged data growth.

6.12.2.17. Contractor shall increase storage, with County approval, in order to meet County business needs.

6.12.2.18. Contractor shall produce monthly Storage Services reports by storage tier down to the Business Group, department and End-User.

6.12.2.19. Contractor shall provide End-User self-service reporting and self-service management for Storage Services.

6.12.2.20. Contractor shall design, deliver, for County approval, and implement centralized control and management for Storage Services.

6.12.2.21. Contractor shall continuously implement plans, approved by the County, to lower storage costs to the County for Storage Services.

6.12.2.22. Contractor shall develop, deliver, for County approval, and implement plans to reduce down time due to data loss for Storage Services.

6.12.2.23. Contractor shall provide secure and bonded transportation and offsite storage of backups.

6.12.2.24. Contractor shall refresh Attached storage on the same cycle as the associated physical server.

6.12.2.25. Contractor shall refresh the Primary, Secondary and Archive tiers of storage on a five (5) year.

6.12.2.26. Contractor shall maximize the efficient use of storage throughout the Data Center Services to minimize and eliminate underutilization.

6.12.3. Environment

County Data included in the Storage Services environment shall be the following:

- County Portfolio Application
- End-User data

6.12.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Storage Services.

Storage Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations on Storage Services architecture.	X	
2. Review and approve recommendations on Storage Services architecture.		X
3. Produce and submit plans on Shared Storage Services consolidation and Application Server migration to Shared Storage Service environment on a yearly basis.	X	
4. Review and approve plans on Shared Storage and Data Management Services consolidation and Application Server migration to Shared Storage Service environment on a yearly basis.		X
5. Produce and submit Storage Services policies/procedures.	X	
6. Review and approve Storage Services policies/procedures.		X
7. Produce and submit Storage Services reporting policies/procedures.	X	
8. Review and approve Storage Services reporting policies/procedures.		X
9. Produce and submit Storage Services policies and procedures.	X	
10. Review and approve Storage Services policies and procedures.		X

Storage Services Roles and Responsibilities		
11. Produce and submit Storage Services refresh plan on a yearly basis.	X	
12. Review and approve Storage Services refresh plan on a yearly basis.		X
13. Produce and submit plans for meeting storage demands.	X	
14. Review and approve plans for meeting storage demands.		X
15. Produce recommendations for process improvement in backup and recovery for Storage Services Assets.	X	
16. Recommend and submit recovery policies/procedures for Storage Services Assets.	X	
17. Review and approve recovery policies/procedures for Storage Services Assets.		X
18. Produce and submit recommendation on capacity management.	X	
19. Review and approve recommendations on capacity management.		X
20. Produce and submit plans to add additional Storage.	X	
21. Review and approve plans to add additional Storage.		X
22. Produce and submit a data management strategy that make certain that commonly used data has a defined minimum set of characteristics that include the following: • Definition of the data object (what is it?) • Reference (where and how is the data object used?) • Metadata (data object attributes, such as type, size, and range of values) • Ownership and governance (who owns data, definitions, content, and so on?)	X	
23. Review and approve data management strategy.		X
24. Implement that strategy using an Information Lifecycle Management (ILM) approach for storing County Data.	X	

Storage Services Roles and Responsibilities		
25. On an initial and ongoing basis, evaluate the County's data to identify redundancies, excess capacity, and opportunities for data consolidation using strategies such as data warehousing and data archiving and reduce data storage costs through the following: • Leveraging centralized hardware • Reducing administrative costs by reducing the number of databases • Providing centralized data repository • Reducing costs by reducing under-utilized storage • Reducing and eliminating autonomous backup and recovery solutions for centrally administered and managed backup and recovery	X	
26. Plan and schedule all storage-related software/driver/microcode/etc. patching and upgrades.	X	
Build Requirements, Roles and Responsibilities	**Contractor**	**County**
27. Design and Implement recovery processes based on approved policies/procedures.	X	
28. Design and Implement Storage Services management processes based on approved policies/procedures.	X	
29. Implement Storage Services Reporting.	X	
30. Design and Implement storage consolidation based on approved recommendations.	X	
31. Deploy, manage, communicate and report on activities related to Storage Services refresh.	X	
32. Review and approve Storage Services refresh report.		X
33. Design and Implement Storage Services provisioning and allocation processes based on approved policies.	X	
34. Design and implement capacity management.	X	
35. Implement approved Storage Services policies and procedures.	X	
36. Implement necessary physical and logical security to protect the County's data (e.g. through access controls, storage network, and host-based allocation controls, SAN zoning and host/array-level logical unit (LUN) masking).	X	
Operate Requirements, Roles and Responsibilities	**Contractor**	**County**

Storage Services Roles and Responsibilities		
37. Provide support, including break-fix, for all Storage Services Assets.	X	
38. 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.	X	
39. Manage and support the Storage Services.	X	
40. Produce and submit monthly Storage Services reports.	X	
41. Review and approve monthly Storage Services reports.		X
42. Support Storage Services refresh.	X	
43. Perform and support media management activities for Storage Services.	X	
44. Manage and support the media requests.	X	
45. Provide data storage Services (e.g., RAID groups, storage pools, LUNs; presenting — masking and zoning; reclamation; optimization — tiers, deduplication, thin provisioning, etc.).	X	
46. Perform tapes mounts as required.	X	
47. Perform special tape shipments as requested.	X	
48. Provide options for on-premises and offsite data backup storage.	X	
49. Provide backup and restore options such as the possibility to self-restore.	X	
50. Load and manage Third-Party media as required.	X	
51. Prepare and manage media for use by microfiche service.	X	
52. Manage and perform file transfers and other data movement activities related to break-fix or consolidation of Storage Services Assets.	X	
53. Perform data backups of Storage Services per approved policies and procedures.	X	
54. Perform recovery processes on Storage Services Assets.	X	
55. Perform storage utilization management.	X	
56. Manage and maintain all Storage Services Assets and Services.	X	

Storage Services Roles and Responsibilities		
57. Manage and maintain backup media library.	X	
58. Manage and maintain the Storage Services Assets.	X	
59. Produce and submit Storage Services Management Reports.	X	
60. Review and accept Storage Services Management Reports.		X

6.13. Backup and Recovery Services

6.13.1. Overview

Backup and Recovery Services are the activities associated with providing ongoing Backup and Recovery according to County schedules and requirements. Contractor must demonstrate that it consistently meets or exceeds County's ongoing Backup and Recovery requirements. All Hardware, all Software and all storage (online, near online, and offline) used for any backup and recovery Services are Contractor-provided.

6.13.2. High Level Requirements

6.13.2.1. Contractor shall perform backups on all County Data.

6.13.2.2. Contractor shall develop management plan that contains procedures for monitoring backup infrastructure, for ensuring successful backup and recovery job completion, for complying with change management process and for testing restore process.

6.13.2.3. Contractor shall maintain a complete inventory of all existing backup equipment including, backup servers and clients, automated libraries, backup media and storage networking components.

6.13.2.4. Contractor shall provide centralized backup and recovery policy management.

6.13.2.5. Contactor shall support disk-based backup target.

6.13.2.6. Contractor shall provide provision for auto discovery of virtual servers.

6.13.2.7. Contractor shall provide single-pass image backup of virtual servers.

6.13.2.8. Contractor shall provide integrated authentication and LDAP services.

6.13.2.9. Contractor shall support Oracle RMAN integration.

6.13.2.10. Contractor shall provide volume shadow copy service (VSS).

6.13.2.11. Contractor shall support full and incremental backups.

6.13.2.12. Contractor shall provide file and virtual server image restore capability.

6.13.2.13. Contractor shall provide ability to customize retention period by policy

6.13.2.14. Contractor shall support application quiesce.

6.13.2.15. Contractor shall support file include/exclude functionality.

6.13.2.16. Contractor shall support data that resides in cloud infrastructure Contractor shall provide point-in-time file and object recovery.

6.13.2.17. Contractor shall perform continuous capacity planning in the Backup and Recovery Services environment to address data growth.

6.13.2.18. Contractor shall implement a NetBackup solution for Tulsa and San Diego sites with replication of immutable copies in Colorado Springs for Disaster Recovery. The Netbackup solution shall also provide daily backup of the AWS West Commercial tennant, with daily replication to the AWS East Commercial immutable tenant for disaster recovery.

6.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Backup and Recovery Services.

Backup and Recovery Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Backup and Recovery schedules, requirements and policies.		X
2. Recommend standard practices for Backup and Recovery Services strategies, policies, and process and procedures.	X	
3. Develop, document and maintain in the Standards and Procedures Manual the Backup and Recovery schedules and procedures that adhere to County requirements and policies.	X	
4. Coordinate the Backup and Recovery Standards and Process and Procedure Manual with County Security and Legal teams.	X	
5. Review and approve Backup and Recovery schedules and process and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
6. Define Backup and Recovery Monitoring and Reporting requirements and policies.	X	
7. Review and approve Backup and Recovery Monitoring and Reporting procedures.		X
Operate Roles and Responsibilities	**Contractor**	**County**
8. Provide and Manage backup media inventory (tape, disk, optical and other media type) including the ordering and distribution of media.	X	
9. Perform Framework Component backups and associated rotation of media as required.	X	
10. Identify and establish a secure off-site location for data media.	X	
11. Approve secure off-site location for data media.		X
12. Archive data media at a secure off-site location.	X	
13. Ensure ongoing ability to recover archived data from media as specified (backward compatibility of newer backup equipment).	X	

Backup and Recovery Services Roles and Responsibilities		
14. Test backup media to ensure incremental and full recovery of data is possible and ensure integrity, as required or requested by County.	X	
15. Recover files, file system or other data required from backup media, as required or requested by County.	X	
16. Provide recovery and backup requirements and updates as they change.		X
17. Provide County access to backup and recovery reporting and monitoring systems and data.	X	

6.14. Managed Print Services

6.14.1. Overview

This is the section pertains to the Managed Print Services Framework Component within the Data Center Framework. The Managed Print Services Framework Component applies to all the Hardware, Software and services needed to maintain and support managed print. Services provided by the Contractor are print and output facilities, print output operations, operating printer devices, distributing printed output, replenishing consumable materials, preparing and managing media for use by microfiche service and repairing printer devices

6.14.2. High Level Requirements

6.14.2.1. Maintain reliable Managed Print Operations that allows County business to continue uninterrupted.

6.14.2.2. Lower overall Managed Print cost by increasing overall efficiencies.

6.14.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Managed Print Services.

Managed Print Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Managed Print Services Roles and Responsibilities		
1. Produce and submit output management requirements, policies, and procedures including transport, delivery locations and schedule requirements.	X	
2. Review and approve output management requirements, policies, and procedures.		X
3. Produce and submit automated output distribution requirements.	X	
4. Review and approve automated output distribution requirements.		X
5. Produce and submit recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.	X	
6. Review and approve recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Design and implement output management requirements, policies, and procedures including transport, delivery locations and schedule requirements.	X	
8. Design, test and implement approved automated output distribution requirements.	X	
9. Design, test and implement approved recommendations for modernizing the Managed Print Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Provide support, including break-fix, for all Managed Print Assets.	X	
11. Provide print output (including both paper and microfiche) facilities for the County.	X	
12. Perform and manage print output (including both paper and microfiche) distribution and delivery to specified County locations.	X	
13. Separate and organize printed output materials (including both paper and microfiche) and place into designated bins at the designated delivery points.	X	
14. Store preprinted check stock in a secure document vault in Contractor secured print facility.	X	

Managed Print Services Roles and Responsibilities		
15. Ensure that output devices are functioning, including performing or coordinating maintenance and meet or exceed Service Levels.	X	
16. Store and manage consumables, such as paper, special forms, check stock, print ribbons, ink, tapes, etc. Ensure that special forms and check stock are current and adequately stocked every Month. Coordinate acquisition of additional materials as needed.	X	
17. Provide microfiche Services.	X	

6.15. Public Key Infrastructure (PKI) Services

6.15.1. Overview

This section pertains to the Public Key Infrastructure (PKI) Services Framework Component of the Data Center Services Framework. PKI Services infrastructure supports and manages all the keys and certificates, the distribution and identification of public encryption keys, enabling End-Users and devices to both securely exchange data, securely connect to the County internal network, digital signatures and verify identity. The PKI Service consists of Hardware, Software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates.

County currently uses Symantec Managed PKI Service to deliver the PKI Service.

6.15.2. High Level Requirements

6.15.2.1. Contractor shall develop additional use cases for the expansion of PKI Services.

6.15.2.2. Contractor shall develop and implement device authentication strategies based on PKI Services.

6.15.2.3. Contractor shall develop and implement End-User authentication methodologies based on PKI Services.

6.15.2.4. Contractor shall use PKI Services for all applications of digital signature.

6.15.2.5. Contractor shall maintain currency on PKI Services.

6.15.2.6. Contractor shall deploy enterprise self-enrollment for PKI Services hosted on the Service Portal.

6.15.2.7. Contractor shall act as the Policy Authority for PKI Services.

6.15.2.8. Contractor shall be responsible for Certificate Practices Statements in the operation of PKI Services.

6.15.2.9. Contractor shall manage the root CA as a public PKI.

6.15.2.10. Contractor shall manage the entire lifecycle of all certificates used in the PKI Service.

6.15.2.11. Contractor shall establish monthly reporting methodology to track usage of certificates across the entire lifecycle.

6.15.2.12. Contractor shall maintain and establish integration with infrastructure supporting the Services (e.g. mobile device management, software distribution, authentication services).

6.15.2.13. Contractor shall maintain a browser agnostic solution for PKI Services.

6.15.2.14. Contractor shall ensure PKI Services is a valid and certified certificate authority externally.

6.15.2.15. Contractor shall maintain an accurate and up-to-date inventory of PKI Services.

6.15.2.16. Contractor shall design and standardize, with County approval, PKI Services.

6.15.2.17. Contractor shall maintain public key certificates for End-Users and devices.

6.15.2.18. Contractor shall maintain a certificate repository.

6.15.2.19. Contractor shall implement certificate revocation procedures and provide key backup and recovery.

6.15.2.20. Contractor shall maintain support for non-repudiation of digital signatures

6.15.2.21. Contractor shall maintain currency on PKI Services to the latest versions and releases.

6.15.2.22. Contractor shall implement automatic update of key pairs and certificates.

6.15.3. Environment

6.15.3.1. Support

The following is a list of items currently supported or future support by PKI Services:

6.15.3.1.1. Secure Remote Access – strong authentication for Remote Access

6.15.3.1.2. Secure network access - transparent authentication to Wi-Fi access points

6.15.3.1.3. Secure E-Mail – digitally signed, encrypted E-Mail Services

6.15.3.1.4. Strong web authentication – authentication services to web apps and pages via browser

6.15.3.1.5. Document signing – digitally signed Adobe PDF documents

6.15.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with PKI Services.

PKI Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop and submit annually additional use cases for the expansion of PKI Services.	X	
2. Review the additional use cases.		X

PKI Services Roles and Responsibilities		
3. Develop and submit device and End-User authentication plans.	X	
4. Review and approve device and End-User authentication plans.		X
5. Develop, maintain and submit operational procedures and End-User instructions.	X	
6. Review and approve operational procedures and End-User instructions.		X
7. Develop and submit plans to integrate PKI Service into E-Mail Services.	X	
8. Review and approve plans to integrate PKI Service into E-Mail Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Implement designs and plans to PKI Services.	X	
10. Implement certificate lifecycle and self-service capabilities on the Service Portal.	X	
11. Implement integration of PKI Service into E-Mail Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
12. Develop and submit monthly reports on PKI Services.	X	
13. Manage CA Root.	X	
14. Support and maintain certificate lifecycle and self-service capabilities.	X	
15. Maintain CSP statements.	X	
16. Maintain currency of PKI Services.	X	
17. Support authentication of mobile devices.	X	
18. Support E-Mail Service use of PKI Services.	X	

7. APPLICATIONS SERVICES

7.1. Overview

Applications Services consists of three separate sets of requirements, roles and responsibilities:

- Applications Maintenance and Operations (M&O) Services – support for Applications in production
- Applications Development Services – development of new software
- Electronic Health Records (EHR) Program Management Services – support for existing EHR and implementation of additional EHR capabilities.

7.2. Application Maintenance and Operations Services

7.2.1. Overview

M&O Services consist of any one-time and ongoing maintenance, operations, support, planning, management, administrative support, oversight, tuning, planning, and any other Services that are either direct or incidental, ancillary, customary, or necessary to perform the activities described below. The Contractor is responsible to support and maintain all environments and systems required to support Portfolio Applications.

7.2.2. High Level Requirements

7.2.2.1. Contractor shall restore Services in accordance with Service Levels.

7.2.2.2. Contractor shall operationally maintain all Portfolio Applications in production with high availability and performance.

7.2.2.3. Contractor shall ensure all maintenance, development and integration activities are aligned with County architecture standards, guiding principles, architecture bricks and patterns.

7.2.2.4. Contractor shall be responsible for performing work on Incidents (e.g. development, test, training, etc.) and production environments, middleware or any needed components to provide M&O Services for Portfolio Applications.

7.2.2.5. Contractor shall maintain accurate and continuous prompt updates to asset and system documentation.

7.2.2.6. Contractor shall ensure cross Framework integration and communication is conducted for Application Incidents, outages, maintenance work, planning purposes and all changes.

7.2.2.7. Contractor shall provide Services in alignment with ITIL and CMMI standards to ensure predictable, repeatable and successful results.

7.2.2.8. Contractor shall implement new patches and versions (within the current release), prioritizing patches that address security vulnerabilities.

7.2.2.9. Reserved.

7.2.2.10. Contractor shall include all services (e.g., labor), software, hardware, and required system environments.

7.2.2.11. Applications M&O Services do not include programming any additional functionality beyond what is included in new patches and dot releases. Contractor shall perform maintenance Services that include Preventative, Adaptive and Perfective Maintenance as described below:

7.2.2.11.1. Preventive Maintenance

Contractor shall perform preventive maintenance Services to diagnose and correct latent defects and other known errors in the Applications. Contractor is required to provide preventive maintenance that covers events that, if not addressed proactively, may affect Applications in production.

7.2.2.11.2. Adaptive Maintenance

Contractor shall perform adaptive maintenance Services so that Application performance is not affected by changes to interfacing Applications or new Applications or packages and infrastructure

changes that, if not addressed proactively, have the potential to impact Applications in production.

7.2.2.11.3. Perfective Maintenance

Contractor shall perform perfective maintenance Services to optimize performance of the Applications, with particular focus on areas including: general performance tuning (e.g., to improve Application response time), database performance tuning (e.g., storage space, query refinement), etc. Tool and script development to make the Maintenance Services more productive or labor saving is also included in this category.

7.2.3. Roles and Responsibilities

Contractor shall perform the Applications M&O Services described in the overview, high level requirements, descriptions and tables in the sections below. The sections below describe in more detail the requirements, roles and responsibilities in the plan, build and operate format for each specific section.

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Application M&O Services requirements and policies.		X
2. Provide recommendations for archiving, performance tuning, patching, database administration, and Application onboarding/retirement.	X	
3. Provide recommendations for preventive, adaptive, and perfective maintenance.	X	
4. Provide recommendations on operational procedures.	X	
5. Review and approve Contractor recommendations on M&O processes, procedures, maintenance (preventive, adaptive, perfective), and Application onboarding/retirement.		X
6. Provide recommendations for upgrade, system changes, Applications architecture changes or anything else that can affect the operational integrity of the Applications.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
7. Provide annual portfolio analytics on production Applications, including technical obsolescence (at a component level, where applicable), defect rates, and costs by Application.	X	
8. Monitor technical trends through independent research; document and report on products and Services.	X	
9. Participate in annual technical and business planning sessions to establish standards, architecture and project initiatives.	X	
10. Define authorization requirements for End-Users, roles, schemas, etc. and approve change requests.	X	
11. Define job schedules for sequencing and run times.	X	
Build Roles and Responsibilities	**Contractor**	**County**
12. Perform pre-production execution simulation.	X	
13. Provide Services in alignment with ITIL, CMMI standards or other leading practices to result in predictable, repeatable, and successful results.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Update the Standards and Procedures Manual with County-approved procedures and standards.	X	
15. Conduct periodic reviews of configuration documentation for accuracy.	X	
16. Provide a documented list of items to be addressed for consideration as part of future upgrades.	X	
17. Validate and provide Application-related Service Desk scripts are updated and accurate.	X	
18. Approve Service Desk script updates.		X
19. Provide planning and schedules for new Applications supported by M&O Services for a system or change placed into production. M&O shall perform M&O Services after the system is placed into production unless otherwise directed by the County.	X	
20. Approve M&O Services to support a new system or change in production.		X
21. Develop and maintain Application version and release Roadmap for all software and tools for each Portfolio Application.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
22. Provide portfolio report for County review of past month Incidents that impacted Application operations.	X	
23. Provide cost and labor hour information at the PA-ID level to facilitate annual portfolio rationalization and support monthly cost allocation to departments.	X	
24. Perform business planning for capacity and performance.		X
25. Provide input into defining requirements for all Applications Development projects to be transitioned to Applications M&O.	X	
26. Recommend potential improvements to Application security architecture.	X	
27. Identify possible product and software tool enhancement opportunities for improved performance and potential cost savings.	X	
28. Recommend potential improvements to Application security.	X	
29. Review and approve improvements to Application security.		X
30. Perform preventive, adaptive and perfective maintenance based on County-approved procedures.	X	
31. Perform archiving, performance tuning, patching, database administration based on County-approved procedures.	X	
32. Perform system log storage and management.	X	
33. Perform root cause analysis resulting from an Incident.	X	
34. Identify and resolve locking conflicts, latch contention, rollback requirements, etc. for all database instances as it pertains to maintenance activities.	X	
35. Retire Applications (performing tasks based on retirement procedures in the Standards & Procedures Manual) as approved by the County.	X	
36. Perform necessary tasks to remedy risks and Incidents identified in the weekly Application and database performance and capacity reports.	X	
37. Create/refresh development/test databases from production data to support O&M activities according to a pre-scheduled cycle.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
38. Monitor and execute production jobs and perform associated interventions (e.g., restarting jobs, re-running jobs.)	X	
39. Review and approve changes that alter or impact the production system and Application.		X
40. Restore Applications following an outage or Incident.	X	
41. Perform triaging and investigation of Incidents regardless of whether these result in an enhancement in the future or impact other Service Frameworks.	X	
42. Perform code fixes to resolve Incidents that stop, slow or hold-up Application processes.	X	
43. Perform general Application administration.	X	
44. Perform routine system patching (e.g., monthly/quarterly/annual) to keep the system current.	X	
45. Perform prompt updates of system documentation.	X	
46. Perform prompt updates of current code in source code repository.	X	
47. Track trends on Incidents to identify systemic Problems to be reported to the County and corrected by the Contractor.	X	
48. Maintain current non-production environments and keep the system operational for M&O requirements.	X	
49. Provide unplanned maintenance including activities to restore service as initiated by Incident tickets that have been initiated by County Users, or Contractor or Third-Parties.	X	
50. Perform 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.	X	
51. Perform triage support by determining if the Incident is an Application Incident vs. another Framework or a Third-Party Incident.	X	
52. Support Incident and Problem management including RCAs.	X	
53. Coordinate with Third-Parties for patch installation and support for restoration of service.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
54. Provide updates to existing documentation regarding steps necessary to restore service.	X	
55. Provision and de-provisioning all and any accounts that are authorized to be created, changed or modified for Portfolio Applications authentication and authorization.	X	
56. Includes Third-Party patch installation and support to restore service, including all patches that address fixes to known defects and associated security vulnerabilities. If a patch only includes new functionality, it shall be installed under Applications Development Services. If a patch includes both known defects/security vulnerabilities and new functionality, it shall be implemented under Applications Maintenance and Operations Services.	X	
57. Participate in change review control board activities.	X	
58. Proactively evaluate, identify and recommend configurations or Changes to configurations to enhance performance.	X	
59. Update and maintain information and data in the Unified Asset Management System.	X	
60. Establish and maintain configuration and system parameters in a consistent manner across like server environments.	X	
61. Execute processes for the proper maintenance and functioning of Interfaces (e.g., initialization parameter, load balancing, tuning, configuration management).	X	
62. Coordinate communications with Third-Parties and manage the information exchange with interfaces.	X	
63. Perform upgrades to Third-Party software or tools, including operating systems or database software.	X	
64. Perform changes to ensure non-production environments are using same versions, updated code and system features as production.	X	
65. Perform regression testing of Application when an enhancement (e.g., service pack release) or change in code is performed.	X	
66. Conduct Application testing in non-production environments.	X	
67. Perform triage to engage Third-Party, troubleshooting, Application of patches and/or other types of fixes.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
68. Maintain and execute a release management schedule.	X	
69. Perform special testing for events, e.g., public holidays, end of financial year, end of calendar year, daylight savings time.	X	
70. Provide, maintain and update the Portfolio Application Identification (PAID) report of active, inactive and inactive-retain Applications.	X	

7.2.4. Application Programming

Application programming Services are the activities associated with the programming, scripting, configuring or customizing of Application modules to support Maintenance and Operations of the production Application Portfolio.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Programming as part of Applications M&O Services.

Application Programming Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Review County's existing technical standards (e.g., naming, JCL, etc.).	X	
2. Recommend programming (coding), development, and technical documentation policies, procedures, and standards for inclusion in the Standards and Procedures Manual.	X	
3. Review and approve overall programming, development, and technical documentation in the Standards and Procedures Manual.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Create working directories to store source code in the enterprise code version manager or repository.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
5. Maintain all current versions of custom code in the approved code repository managed by the Contractor.	X	

Application Programming Services: Plan, Build and Operate Roles and Responsibilities		
6. Recommend modifications and performance-enhancement adjustments to system software and utilities based on County performance standards.	X	
7. Manage all programming and development efforts using industry-standard project management tools and methodologies.	X	
8. Perform all software engineering activities using industry best practices.	X	
9. Employ standard software engineering practices to promote consistency and maintainability.	X	
10. Conduct planned status reviews and provide written report on results to County.	X	

7.2.5. Application Integration and Testing

Application integration and testing are the Services associated with the confirmation that the individual Application Framework Components work together properly and, as a whole, perform their specified functions. This includes Interfaces to other Applications already in production at, or developed by, County or Third-Parties as stated in the applicable requirements documents.

The following table identifies the Application Integration and Testing Services that the Contractor shall perform.

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop, document and maintain in the Standards and Procedures Manual integration and testing procedures that meet County requirements and adhere to policies defined by County.	X	
2. Review and approve changes to the Standards and Procedures Manual for testing.		X
3. Develop an overall test plan that documents the test strategy, coverage, scenarios, test bed, test data, methods, schedule and responsibilities to accomplish integration and testing.	X	
4. Approve test plan.		X
Build Roles and Responsibilities	**Contractor**	**County**

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
5. Provide a test bed with real-time production data.	X	
6. Mask sensitive information in tests that use production data.	X	
7. Create test cases with appropriate use of County-provided data for generating test data to perform all appropriate testing, e.g., unit testing, end-to-end testing, stress testing, regression testing.	X	
8. Create test scenarios to test end-to-end business cases.	X	
9. Create test environment and data where required for support, enhancements or projects, including demonstration of requirements traceability to verify requirements have been satisfied.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Conduct testing per test plan requirements.	X	
11. Facilitate and support User acceptance test as agreed-upon with the County, e.g., establish adequate test environment based on User acceptance criteria, prepare data to support test scenarios within modified system, manage the relationship with all interfaced systems necessary to conduct test, perform troubleshooting, simulate interfaces or working with integrated systems to conduct end-to-end testing, support batch processing, exercise functionality and report results.	X	
12. Conduct User acceptance test.		X
13. Manage the County functional, Integration test, and Regression Testing environments and associated test data, including creation and maintenance during the testing period.	X	
14. Provide shared access to the mutually agreed-upon defect tracking tool for the purpose of allowing County to initiate, track, and report County-identified defects (e.g., User acceptance testing).	X	
15. Correct defects found as a result of testing efforts.	X	
16. Stage systems before implementation into production.	X	
17. Support County for functional and non-functional testing of Applications to confirm systems are functioning as expected after infrastructure changes have been implemented.	X	
18. Maintain software release matrices across development, quality assurance and production environments and networks.	X	

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
19. Conduct Integration test and security testing for all new and upgraded Application software, including the associated equipment and networks to include Unit testing, system, Integration test and Regression testing based on requirements defined in requirements and design documents.	X	
20. Assess and communicate the overall impact and potential risk to components prior to implementing Changes.	X	
21. Stage new and upgraded software or services to seamlessly transition into existing environment based on requirements defined in requirements and design documents.	X	
22. Perform Configuration Management and Change Management activities related to integration and testing.	X	
23. Review and approve test results.		X
24. Manage and support software and test data in test environments.	X	
25. Ensure testing results are in compliance with policies, procedures, plans, and test criteria and metrics (e.g., defect rates, progress against schedule).	X	
26. Define test-to-production turnover requirements and instructions for each Project or release.	X	
27. Approve test-to-production turnover requirements and instructions.		X
28. Produce and submit reports on results from test-to-production activities if applicable.	X	
29. Review and approve reports on test-to-production results.		X
30. Perform software support to migrate code from test to production as approved by the County.	X	
31. Track migration status and notification.	X	

7.2.6. Application Implementation and Data Migration

Application implementation and data migration Services are the activities associated with the installation and migration of new or upgraded components to the production environment. In addition, these include Services to localize new or upgraded components so that they adhere to local business practices as well as legal, regulatory and statutory needs.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Applications that receive patches, version upgrades, or other changes.

Application Implementation and Data Migration Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Create an implementation plan outlining the scope, approach and execution planned for the deployment of new/enhanced Applications and/or the migration of Applications into M&O Services.	X	
Build Roles and Responsibilities	**Contractor**	**County**
2. Perform data migration from existing systems to new systems, by either electronic or manual methods.	X	
3. Produce and submit operations and administration procedures related to code migration (e.g. CRCB documents, code version check in, etc.).	X	
4. Review and approve operations and administration procedures related to code migration.		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Coordinate and assist with deployment and support activities with County and/or its designees as directed by County.	X	
6. Develop data migration plans and scripts for use or execution by County, whether from existing systems to new systems, by either electronic or manual methods as required.	X	
7. Execute data migration plan by moving data into the production environment.	X	
8. Develop, document and maintain in the Standards and Procedures Manual implementation and migration procedures that meet requirements and adhere to policies defined by County.	X	
9. Coordinate and review all implementation and migration plans, in accordance with Change Management policies.	X	
10. Upon County request and approval install new or enhanced components (e.g., software, middleware, utilities, configurations) within the development environment.	X	

Application Implementation and Data Migration Services: Plan, Build and Operate Roles and Responsibilities		
11. Upon County approval, within the development environment, perform Application Services Framework Component upgrades as a result of new and enhanced architectures and County upgrade plans and requirements (e.g., Hardware, Software, middleware, utilities, networks, peripherals, configurations).	X	
12. Coordinate implementation and migration support activities with County.	X	
13. Within the development environment, perform Application and/or data migration and conversion by electronic or manual methods (e.g., upgraded databases, address tables, management information bases).	X	
14. Attend and seek change control review board approval, or any other procedures required to obtain approval to implement a change into production environment.	X	
15. Create "go-live" checklist and conduct the "go/no-go" meetings	X	
16. Approve production implementation, go-live checklist and "go/no-go" decisions.		X
17. Deploy system.	X	

7.2.7. Application Documentation

Contractor shall develop and maintain documentation for all Applications, including:

- System specifications and documentation
- Solution design documentation
- System security plans
- End-User documentation
- Updates and release notes
- Run-book data and documentation

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Applications Documentation.

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
1. Recommend specifications and documentation format and content per County requirements.	X	
2. Approve documentation format and content.		X
3. Provide system specifications and technical documentation.	X	
4. Provide operational processing flow.	X	
5. Provide system installation, support, configuration and tuning documentation.	X	
6. Provide Application hardware and system Software requirements documentation.	X	
7. Provide documentation for Applications on patches, updates and release notes.	X	
8. Provide solution design documentation.	X	
9. Review and approve all Applications documentation.		X
Build Roles and Responsibilities	**Contractor**	**County**
10. Maintain, and provide County access to, physical and logical on-line libraries of all deliverables and documentation produced in the course of performing Applications work (e.g., specifications, process flows, User manuals, operating manuals).	X	
11. Prompt update documentation to be current and accurate in all relevant system of records (e.g., AppsManager, Service Desk Scripts, Solution Design Documents).	X	
12. Prompt update of code version manager tool set with updated code that is created or changed. The code repository managed by the Contractor must be accurate and current.	X	
13. Validate documentation is promptly updated and coding standards are followed.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide system and Application security procedures.	X	
15. Provide standard operating procedures in support of Application characteristics and features.	X	
16. Prepare updates and release notes.	X	
17. Document version control for all documentation.	X	

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
18. Assist County in developing an Application Disaster Recovery process and the associated documentation.	X	
19. Approve documentation.		X

7.2.8. Application Training

Following Transition and after each implementation, Contractor shall conduct all the necessary training programs for Contractor Personnel to preserve and enhance the knowledge and understanding of the Applications. It is the Contractor's responsibility to maintain this proficiency for replacement Contractor Personnel at no additional cost to the County. Contractor shall provide base training to key County personnel when Contractor develops a new functionality.

Contractor shall share with County the experience that Contractor has gained from daily Incident handling via knowledge sharing sessions, best practices sessions, training programs, etc., to improve the overall knowledge base of the Applications. Contractor shall provide County with copies of all instructor manuals and other training materials created or used by Contractor Personnel in conducting such training.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Training.

Application Training Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop training plan.	X	
2. Approve training plan.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Update technical training materials.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide technical training assistance and knowledge transfer to existing County support personnel, during deployment as requested.	X	
5. Provide training materials related to the technical aspects of Applications to County as applicable.	X	

Application Training Services: Plan, Build and Operate Roles and Responsibilities		
6. Support County's training of its Service Desk agents, including supporting County's development of dialogue scripts.	X	
7. Develop, document and maintain in the Policies and Procedures Manual Training and knowledge transfer procedures that meet County's requirements and adhere to policies defined by County.	X	
8. Develop and deliver training program to instruct County personnel on the provisions included within the Services (e.g., "rules of engagement," how to request Services).	X	
9. Develop and implement knowledge transfer procedures so that key County staff understand key components of the Enhancements and/or Deliverables.	X	
10. Develop, document and deliver training requirements that support the ongoing provision of the Services, including refresher courses as needed and instruction on new functionality.	X	

7.2.9. Application Quality Assurance Services

Contractor shall provide the Quality Assurance (QA) Services with respect to all Applications created or enhanced as part of this Agreement. QA Services are a systematic, planned set of actions necessary to provide confidence that the Software update/development processes conform to established functional technical requirements as well as with the managerial requirements of keeping the schedule and resources within budgetary confines. Contractor shall provide County with appropriate visibility into the QA Services processes that Contractor uses and of the results as related to the Application being worked upon.

Contractor shall support and suggest improvements for all QA Services conducted and processes adopted by County.

Contractor shall perform the QA Services throughout the entire Software Development Life Cycle (SDLC). QA Services include the following:

- A quality management approach
- Effective software engineering technology (methods and tools)
- Formal technical reviews applied throughout the SDLC process
- A multi-tiered Application integration and testing strategy, and implementation
- Control of software documentation and associate changes

- A procedure to measure compliance with software development standards
- Measurement and reporting mechanisms

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Quality Assurance.

Application Quality Assurance Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Create and submit a quality management approach to be updated in the Standard and Procedures Manual.	X	
2. Review and approve quality management approach.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Perform formal technical reviews applied throughout the SDLC process.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide QA measurements and reporting.	X	

7.2.10. Database Administration

Database Administration Services are the activities associated with the maintenance and support of production databases. This includes responsibility for managing data, monitoring the database, routine maintenance, database log file reviews, dataset placement, database performance, and data recovery and integrity at a physical level.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Database Administration.

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Database administration requirements and policies including authorization requirements for End-Users, roles, schemas, etc., and approve Change requests.		X
2. Develop and document in the Standards and Procedures Manual Database Administration procedures that meet requirements and adhere to defined policies.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
3. Review and approve Database Administration procedures.		X
4. Develop and provide database roadmaps for version releases for planning and Portfolio Management.	X	
Build Roles and Responsibilities	**Contractor**	**County**
5. Provide security administration including managing role and End-User database permissions in accordance with County policies.	X	
6. Perform database restores from export dumps or backups.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Create/refresh development/test/QA databases from production data.	X	
8. Execute authorization Service Requests.	X	
9. Define and provide database creation, configuration, upgrade, patches and refresh requirements.		X
10. Execute database creation, configuration, upgrades, patches and refresh.	X	
11. Execute all database system-level changes (e.g., initialization parameters).	X	
12. Execute all schema changes for all instances.	X	
13. Execute database data definition requirements for Applications (IMAR for tables, triggers, attributes, etc.).	X	
14. Maintain documentation for all database instance parameters and system settings.	X	
15. Maintain consistent database parameters and system settings across all like instances; consistency must be maintained according to established development to QA to production life cycle.	X	
16. Execute database data definitions for Applications and developer schemas.	X	
17. Define and execute database performance and tuning scripts, and keep database running at optimal performance for County's workload.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
18. Implement and administer appropriate database management tools across all database instances. Performance metrics and historical data must be available for trending and reporting over a minimum of 6 months.	X	
19. Identify and resolve locking conflicts, latch contention, rollback requirements, etc., for all database instances.	X	
20. Provide technical assistance and subject matter expertise to County Application developers and Third-Party support.	X	
21. Provide data dictionary expertise, End-User data assistance, Data Warehouse Metadata definition, data mapping functions.	X	
22. Monitor database and generate automatic Service Desk trouble tickets for Incidents.	X	
23. Patch database software as needed according to established development to QA to production life cycle.	X	
24. Manage database communication software configuration, installation and maintenance.	X	
25. Provide database storage management and cleanup activities.	X	
26. Define database backup schedules, retention periods, levels (i.e., full, incremental or differential).		X
27. Execute County's database backup and recovery policies.	X	
28. Deliver backup and restore activities for support and/or as requested via Service Request.	X	
29. Provide database capacity management and availability management. Examples of activities include failover testing, monitoring, performance planning, etc.	X	
30. Maintain storage allocation, file systems and current usage, file system and capacity management.	X	
31. Provide database installation, de-installation and administration, testing, copying, and security and User management.	X	
32. Provide administrative account support.	X	
33. Provision and de-provision all and any accounts that are authorized to be created, changed or modified.	X	
34. Provide system monitoring and documentation	X	
35. Maintain transactional logs and backup upon set schedule.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
36. Provide operational support of County's public or private cloud databases.	X	

7.3. Application Development Services

7.3.1. Overview

Application Development Services shall apply to functional changes within the existing Application portfolio and any new Application development activities.

7.3.2. High Level Requirements

7.3.2.1. Contractor shall perform all development and integration activities in alignment with the County IT Strategic Plan and strategic roadmaps.

7.3.2.2. Contractor shall ensure integration with existing data or Applications is scoped and delivered per the requirements.

7.3.2.3. Contractor shall ensure all development activity follows the County's Information Technology standards, guiding principles, architecture bricks and patterns.

7.3.2.4. Contractor shall provide technology assistance and support to the County in planning and standard setting activities.

7.3.2.5. Contractor shall create and maintain accurate and continuous prompt updates to be added to the asset and system documentation.

7.3.2.6. Contractor shall ensure cross Framework integration and communication is conducted for Application development requiring cross Framework integrations.

7.3.2.7. Contractor shall provide Services in accordance with ITIL and CMMI standards to ensure practices result in predictable, repeatable, and successful results.

7.3.2.8. Contractor shall review and comply with all County existing technical standards (e.g., naming, JCL, etc.).

7.3.2.9. Contractor shall provide Application integration and testing to confirm that the individual Application Framework Components work together properly and, as a whole, perform their specified functions.

7.3.2.10. Contractor shall provide integration and testing of Interfaces to other Applications already in production at, or developed by, County or Third-Parties as stated in the applicable requirements documents.

7.3.2.11. Contractor shall provide Application data migration associated with the installation and migration of new or upgraded components to the production environment.

7.3.2.12. Contractor shall provide base training to key County personnel when Contractor develops a new functionality.

7.3.2.13. Contractor shall validate that all the activities necessary to design, develop and implement any development or changes are not only effective and efficient for quality assurance and control but geared toward continuous quality improvement.

7.3.2.14. Contractor shall perform QA Services throughout the entire Software Development Life Cycle (SDLC). QA Services include the following:

- A quality management approach
- Effective software engineering technology (methods and tools)
- Formal technical reviews applied throughout the SDLC process
- A multi-tiered Application integration and testing strategy, and implementation
- Control of software documentation and associate changes
- A procedure to measure compliance with software development standards

- Measurement and reporting mechanisms

7.3.2.15. Contractor shall ensure and meet all requirements to transition from Applications Development into Applications Maintenance and Operations support when placed into production status.

Contractor shall perform the Applications Development Services described in the overview, high-level requirements, descriptions and tables in the sections below, as well as the Applications Common Services described below. The sections directly below describe in more detail the requirements, roles and responsibilities in the Plan, Build and Operate format for each specific section.

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop Application architecture and future roadmap.	X	
2. Create and deliver high-level Application solution design document, including architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).	X	
3. Identify requirements for Disaster Recovery and Business Continuity Planning.	X	
4. Identify security requirements, risks or vulnerabilities in any solution provided as part of Applications Development and provide plans to address or mitigate.	X	
5. Develop plan and approach to migrate developed Application to M&O Services, including warranty services (if applicable).	X	
6. Review and approve plan and approach to migrate developed Application to M&O Services.		X
7. Participate in periodic technical and business planning sessions to establish standards, architecture, and project initiatives.	X	
Build Roles and Responsibilities	**Contractor**	**County**
8. Review project scope of work to assess alignment with architecture standards, provide recommendations.	X	
9. Assess impacts and linkages to other Applications.	X	

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
10. Develop detailed solution design documentation, including environment configuration, integration requirements and technical details.	X	
11. Review and approve detailed solution design documentation.	X	
12. Recommend implementation alternative approaches.	X	
13. Review and approve implementation approach.	X	
14. Provide updates to Application architecture documents based on as-built development activities.	X	
15. Provide Budget Estimates upon request by the County.	X	
16. Provide Service Request Project Estimates upon request by the County.	X	
17. Review and approve Service Request Project Estimates.		X
18. Assist with development of business requirements as requested by the County.	X	
19. Assist with development of technical statements of work for Application systems as requested by the County.	X	
20. Review and approve business requirements and Applications technical statements of work.		X
21. Assess capacity, availability, and performance impacts for recommended solutions.	X	
22. Identify and communicate any impacts to the Service Request project cost and schedule estimate.	X	
23. Review and approve revised Service Request project cost and schedule estimate.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
24. Alert County to exceptions in architecture standards.	X	
25. Review and approve architecture standard exceptions.		X
26. Identify and document risks/challenges with recommended solution.	X	
27. Monitor technical trends through independent research, and document and report on products and services with applicability to the County.	X	

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
28. Recommend SDLC process improvements, and document in Standards & Procedures Manual if approved by the County.	X	
29. Support market scans upon request to explore Third-Party solutions.	X	
30. Conduct/coordinate Application evaluations of new products/services.	X	
31. Evaluate and recommend upgrade process for new Application system versions.	X	
32. Develop and communicate risk assessment for development efforts and implementation.	X	
33. Develop project plan, including cost and schedule estimates.	X	
34. Review and approve project plan, including cost and schedule estimates.	X	
35. Develop logical and physical data models.	X	
36. Develop and maintain requirements traceability matrix.	X	
37. Develop prototype Applications to evaluate functionality, requirements.	X	
38. Ensure updates are made to Applications repositories, Configuration Management, and Asset Management.	X	
39. Adhere to Release Management policies/procedures.	X	
40. Develop Application functional requirements documents and conceptual data models.	X	
41. Review and approve functional requirements and conceptual data models.		X

7.4. Electronic Health Records (EHR) Program Management Services

7.4.1. Overview

7.4.1.1. EHR Program Management Services support the use of existing EHR and implementation of additional EHR capabilities to meet operational needs. EHR Program Management Services shall have

a designated EHR Program Manager under the Agreement and will be staffed accordingly.

7.4.1.2. EHR Program Management Services shall be provided to various Health and Human Services Agency (HHSA) programs including but not limited to HHSA Information Technology Services (ITS) and staff and contractors involved in the implementation and/or support of clinical systems in HHSA.

7.4.2 High Level Requirements

7.4.2.1 Contractor shall engage a qualified EHR Program Manager.

7.4.2.2 The EHR Program Manager shall work with HHSA Director, ITS and/or other leader(s) designated by the HHSA Director.

7.4.2.3 The EHR Program Manager shall develop technical program/project management best practices/templates and provide training/mentoring to project teams.

7.4.2.4 The EHR Program Manager shall monitor dependencies across multiple interrelated technical projects.

7.4.2.5 The EHR Program Manager shall gather and report consolidated technical project status and financial information to HHSA leadership.

7.4.2.6 The EHR Program Manager shall assist a central governing body to review/audit adherence to methodologies, budgets, and timing.

7.4.2.7 The EHR Program Manager shall assists HHSA leadership in managing EHR projects/programs.

7.4.2.8 The EHR Program Manager shall oversees short to mid-term (1-3 years) EHR strategy execution and operations in alignment with HHSA objectives.

7.4.2.9 The EHR Program Manager shall provide oversight of multiple concurrent clinical systems projects.

7.4.2.10 The EHR Program Manager shall makes decisions which have a serious impact on the overall success or failure on area of accountability.

7.4.2.11 The EHR Program Manager shall collaborate with project managers and business sponsors to ensure value delivery.

7.4.2.12 The EHR Program Manager shall provide recommendations, performance metrics, and measurements based on HHSA goals.

7.4.2.13 The EHR Program Manager shall monitor project portfolio reporting and provide program-level reporting to stakeholders.

7.4.2.14 The EHR Program Manager shall gather, manage, and prioritize high-level operational requirements to be leveraged in the development of solutions to meet HHSA business needs.

7.4.2.15 The EHR Program Manager shall advise and support HHSA stakeholders on Contractor's processes and standards.

7.4.2.16 The EHR Program Manager shall coordinate work request submissions.

7.4.2.17 The EHR Program Manager shall maintain list of HHSA clinical system projects and priorities.

7.4.2.18 The EHR Program Manager shall perform a monthly program review to include a summary of program management activities, relay HHSA requests, review active project log and status, and identify Contractor support needs for upcoming projects.

END OF SCHEDULE