Problem Resolution Report

CoSD Contract No. 554833
Cloud IaaS and PaaS Resource Unit
Perspecta/CoSD 083

perspecta

Date: November 18, 2020

Summary:

In accordance with the provisions of the IT and Telecommunications Service Agreement No. 554833 (the "Agreement") by and between the County of San Diego ("County") and Perspecta Enterprise Solutions LLC ("Perspecta" or "Contractor" and hereinafter collectively referred to as "the Parties"), agreement is reached on the Effective Date shown below.

Issue or Problem:

As new applications are implemented in the Cloud (e.g. IPTS) and existing applications (e.g. MEGA) are transitioned from the Data Center to the Cloud, the Parties need a pricing methodology for the services provided by Cloud providers and Contractor.

Resolution:

1. The Parties agree that the Data Center Services Framework includes Cloud services. The Contractor's obligations (e.g., liability, service levels, disentanglement) under the Agreement applies to Cloud services.

2. The Parties agree to adopt an interim pricing approach for applications which are already or will be hosted in either Amazon Web Services (AWS) or Microsoft Azure (MS Azure). The interim pricing approach, as described in this PRR will be effective 07/01/2020; however, negotiations on any changes to the approach for 7/1/2021 and beyond, including RU pricing, will be completed no later than 12/15/2020 in order to provide budget guidance to County departments for Fiscal Year 21-22.

3. As part of the interim pricing approach, the Parties agree to establish the following RUs:

    a. ***Virtual Server - Cloud IaaS*** with a corresponding RU Fee of $551.27 for the support services provided by Contractor for each Infrastructure as a Service (IaaS) instance in the AWS and MS Azure clouds.

    IaaS includes compute, storage and container management services.

    b. ***Virtual Server - Cloud PaaS*** with a corresponding RU Fee of $413.45 for the cost of the support services provided by Contractor for each Platform as a Service (PaaS) instance in the AWS and MS Azure clouds.

    PaaS provides cloud components (e.g., database server, web server) for certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications.

4. Also, as part of the interim pricing approach, AWS and MS Azure services will be billed as actuals plus a 5% markup. This cost is variable and are based on consumption. Contractor's MS Azure CSP discount will be equally allocated between Contractor and County.

5. Schedule 16.1 of the Agreement is amended by adding Section 12.4 - Cloud Services as per Attachment 1 to this PRR.

6. Schedule 4.3 of the Agreement is amended by updating sub sections 6.1 – 6.4, as per Attachment 2 to this PRR.

7. Exhibits 16.1-1, 16.1-2 and 16.1-6 to the Agreement are amended by adding the Virtual Guest Server – Cloud IaaS RU and the Virtual Guest Server – Cloud PaaS RU, as per Attachment 3, 4 and 5, to this PRR.

****

The resolution of the issue or Problem as described in this Problem Resolution Report shall govern the Parties' actions under the Agreement until a formal amendment of the Agreement is implemented in accordance with the terms of the Agreement, at which time this Problem Resolution Report shall be deemed superseded and shall be null and void.
All other terms and conditions of the Agreement remain unchanged and the Parties agree that such terms and conditions set forth in the Agreement shall continue to apply. Unless otherwise indicated, the terms used herein shall have the same meaning as those given in the Agreement.

IN WITNESS WHEREOF, The Parties hereto, intending to be legally bound, have executed by their authorized representatives and delivered this Problem Resolution Report as of the date first written above.

COUNTY OF SAN DIEGO		**PERSPECTA ENTERPRISE SOLUTIONS LLC**	
By:		By:	
Name:	John M. Pellegrino	Name:	Max Pinna
Title:	Director, Department of Purchasing and Contracting	Title:	Contracts Manager
Effective Date:		Date:	November 18, 2020

12.4 Cloud Services

This section pertains to the Fees associated with Cloud Services infrastructure support for applications hosted in either Amazon Web Services (AWS) or Microsoft Azure (MS Azure). Contractor shall administer and manage AWS and MS Azure to meet the requirements described in Schedule 4.3 and Schedule 4.8. Contractor will bill the County the applicable fixed monthly Resource Unit Fee for this service, as listed in Exhibit 16.1-1 and described below:

12.4.1 **Cloud Infrastructure as a Service (IaaS)** is for the support services provided by Contractor for each Infrastructure as a Service (IaaS) instance in the AWS and MS Azure clouds. Contractor shall provide the following support for IaaS: Software License / Maintenance (Operating System, Monitoring, Patching, Discovery, Antivirus); Build; Monitoring; Patching; Quality Control; Problem/Incident/Change Management; Upgrades; Decommission; Tech Refresh; Tools Management/Configuration; Server Security; Support to Applications, Service Level support; and Support to Architecture and Engineering.

12.4.2 **Cloud Platform as a Service (PaaS)** is for the support services provided by Contractor for each Platform as a Service instance in the AWS and MS Azure clouds. Contractor shall provide the following support for PaaS: Software License / Maintenance (Monitoring and Discovery); Build; Monitoring; Quality Control; Problem/Incident/Change Management; Decommission; Tools Management/Configuration; Server Security; Support to Applications, Service Level support; and Support to Architecture and Engineering.

Contractor will also bill the County for the services provided by AWS and MS Azure plus a markup of 5%. These services are based on consumption based and therefore variable.

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	

Data Center Services Roles and Responsibilities		
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
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	

Data Center Services Roles and Responsibilities		
28.		
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	
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	

Data Center Services Roles and Responsibilities		
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**
45. Publish all Data Center Services asset standards on the Service Portal.	X	
46. Provide support, including break-fix, for all Data Center Services Assets.	X	
47. Perform maintenance activities during non-peak 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	

Data Center Services Roles and Responsibilities		
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	
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	

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	
1. Review and approve Security architecture for Data Center Services.		X
2. Develop and submit plans for pre-release of Portfolio Applications or any other data center changes scan and vulnerability analysis.	X	
3. Review and approve plan for scan and vulnerability analysis.		X
4. Develop and submit annual operational procedures for data center Security Services.	X	
5. Produce and submit methodology and performance tools to assess and remediate data center security Incidents.	X	
6. Review and approve methodology and performance tools to assess and remediate data center security Incidents.		X
7. Develop and submit design and plans for SIEM tool.	X	
8. Review and approve design and plans for SIEM tool.		X
9. Produce and submit monitoring and managing of all Security Services Hardware and Software.	X	
10. Review and approve monitoring and managing of all Security Services Hardware and Software.		X
11. Produce and submit annual refresh plans for Security Services.	X	
12. Review and approve submit annual refresh plans for Security Services.		
13. Produce and submit security plan for cloud-based services used in hybrid mode.	X	

Security Services Roles and Responsibilities		
14. Review and approve security plan for cloud-based services used in hybrid mode.		X
15. Produce and submit lock-down scripts for Data Center Services.	X	
16. Review and approve lock-down scripts for Data Center Services.		X
17. Develop process to continuously post all documentation developed and maintained in Security Services to the Service Portal.	X	
Build Roles and Responsibilities	**Contractor**	**County**
18. Implement and maintain security architecture in Data Center Services.	X	
19. Develop monthly reports on SIEM and other Incidents affecting security in Data Center Services.	X	
20. Implement single pane management console for Security Services.	X	
21. Perform refresh according to the approved annual refresh plans for Security Services.	X	
22. Implement and monitor security plan for cloud-based services used in hybrid mode.	X	
23. Implement lock-down scripts for Data Center Services.	X	
24. Design, test and implement all policies needed to provide Security Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
25. Review and analyze SIEM activity and report findings monthly.	X	
26. Recommend changes based on operational experiences to the security architecture supporting Security Services.	X	
27. Support all Data Center Services Incidents.	X	
28. Support all Severity 1 Incidents.	X	
29. Continuous review data center for vulnerabilities and recommend corrections promptly.	X	
30. 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.

6.7.3. 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(s) 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	
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

Application Infrastructure Services Roles and Responsibilities		
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	
Build Roles and Responsibilities	**Contractor**	**County**
22. Provide all design and engineering required to deploy, refresh and support Application Infrastructure Services Assets.	X	
23. Design, test and implement hardware standards for Application Infrastructure Services Assets.	X	
24. Design, test and deploy operating system standards for Application Infrastructure Services Assets.	X	
25. Deploy, manage, communicate and report on activities related to Application Infrastructure Services refresh.	X	
26. Review and approve reports on Application Infrastructure Services refresh.		X

Application Infrastructure Services Roles and Responsibilities		
27. Design, test and execute Application Infrastructure Services storage migration and consolidation plan.	X	
28. Implement approved backup/recovery policies and procedures.	X	
29. Design, test and deploy approved Application Infrastructure Services consolidation plans.	X	
30. Test and deploy approved updates or patches to Application Infrastructure Services Assets.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
31. Provide support for Application Pre-Production and Application Test Servers.	X	
32. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or break-fix activity.	X	
33. Monitor, operate, maintain and support the Third-Party Applications running on Application servers.	X	
34. Provide automated event monitoring tools that notify Applications Team for immediate response if there is an application-related Incident.	X	
35. Provide support, including break-fix, for all Application Infrastructure Services Assets.	X	
36. Provide support for Application Infrastructure located in County Locations.	X	
37. Provide support for Application Infrastructure Services storage migration and consolidation plan.	X	
38. Perform backups on Application Infrastructure Services Assets as defined.	X	
39. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or break-fix activity.	X	
40. Support send and receive electronic data transmissions (e.g., EDI, FTP).	X	
41. Perform upgrades to Application Infrastructure Services Assets.	X	
42. Monitor, operate, maintain and support OS (Operating Systems) installed on Application Infrastructure.	X	
43. Monitor, operate, maintain and support the Third-Party Applications running on Application Infrastructure.	X	

Application Infrastructure Services Roles and Responsibilities		
44. Execute standard operating procedures at scheduled times.	X	
45. Start-up and shut-down County online/interactive systems according to defined schedules or upon approved requests.	X	
46. Coordinate and manage Third-Party hardware and software maintenance to meet County requirements.	X	
47. Ensure that System management and monitoring tools do not impact County operations.	X	
48. Provide automated event monitoring tools that shall notify Applications Team for immediate response if there is an application-related 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

Development and Test Services Roles and Responsibilities		
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
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	

Development and Test Services Roles and Responsibilities		
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	
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.

6.10.3. 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	

Storage Services Roles and Responsibilities		
10. Review and approve Storage Services policies and procedures.		X
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.

6.13.3. 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	
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	

Backup and Recovery Services Roles and Responsibilities		
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**
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

Managed Print Services Roles and Responsibilities		
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	
15. Ensure that output devices are functioning, including performing or coordinating maintenance and meet or exceed Service Levels.	X	

Managed Print Services Roles and Responsibilities		
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**

PKI Services Roles and Responsibilities		
1. Develop and submit annually additional use cases for the expansion of PKI Services.	X	
2. Review the additional use cases.		X
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	

PRR 083 - Cloud Services - Attachment 3
Exhibit 16.1-1 - Resource Unit Price Summary

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee	Baseline Annual Fee	RU Fee (70 % to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Fee Per Unit		Specific	48	$ 551.27	$ 26,460.96	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Fee Per Unit		Specific	48	$ 413.45	$ 19,845.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a

PRR 83 - Cloud Services - Attachment 4
Exhibit 16.1-2 - Resource Unit Price Decomposition

Resource Unit	*Reference	Unit of Measure	Pricing Method	Decomposition	Resource Unit Fee	Component Fee	Component Description
Virtual Guest Server - Cloud IaaS	**Schedule 4.3 - Section 6**	**Server**	**Fixed Monthly Per Unit**		**$ 551.27**		
				Hardware		$ -	N/A
				Operating System License		$ 38.59	Represents the cost of software license upgrades/refresh.
				Other Software License		$ 27.56	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 485.12	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Cloud PaaS	**Schedule 4.3 - Section 6**	**Server**	**Fixed Monthly Per Unit**		**$ 413.45**		
				Hardware		$ -	N/A
				Operating System License		$ -	N/A
				Other Software License		$ 20.67	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 392.78	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.

PRR 083 - Cloud Services - Attachment 5
Exhibit 16.1-6 - Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Fee Per Unit		Specific	48	$ 534.73	$ 25,667.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Fee Per Unit		Specific	48	$ 401.05	$ 19,250.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a