

SCHEDULE 4.3 — OPERATIONAL SERVICES

## TABLE OF CONTENTS

<b>SCHEDULE 4.3 — OPERATIONAL SERVICES .....</b>	<b>1</b>
<b>1. Overview of Services .....</b>	<b>4</b>
1.1. Overview .....	4
1.2. High Level Requirements.....	4
1.3. Service Environment .....	4
<b>2. Help Desk Services.....</b>	<b>7</b>
2.1. Help Desk Services Overview.....	7
2.2. Help Desk Services High Level Requirements .....	7
2.3. Help Desk Services Requirements, Roles and Responsibilities.....	7
<b>3. Application Services .....</b>	<b>11</b>
3.1. Application Services Overview.....	11
3.2. Application Services High Level Requirements .....	11
3.3. Application Services High Scope of the Environment.....	11
3.4. Application Services Requirements, Roles and Responsibilities.....	14
<b>4. Desktop Services .....</b>	<b>20</b>
4.1. Desktop Services Overview .....	20
4.2. Desktop Services High Level Requirements.....	21
4.3. Desktop Services Requirements, Roles and Responsibilities .....	21
4.4. Personal Computing Services.....	26
4.5. Video Streaming and Archiving Services .....	38
4.6. Video Conferencing Services.....	39
4.7. Audio/Video Services .....	42
4.8. Catalog Services.....	42
4.9. Network Printer Services .....	46
4.10 Desktop Engineering Services.....	45
4.11 Mobile Device Management.....	45
<b>5. Network Services .....</b>	<b>53</b>
5.1. Network Services Overview.....	53
5.2. Network Service High Level Requirements.....	53
5.3. Network Services Requirements, Roles and Responsibilities.....	55
5.4. Data Network Services.....	57
5.5. Remote Access Services.....	61
5.6. Voice Services.....	62
5.7. Security Services .....	68

*Schedule 4.3 – Operational Services*

---

5.8.	New Site Installation Services.....	72
5.9.	3 <sup>rd</sup> Party Network Access Services .....	73
5.10.	Wireless Access Services .....	76
5.11.	Mobility VPN Access Services .....	79
<b>6.</b>	<b>Data Center Services .....</b>	<b>81</b>
6.1.	Data Center Services Overview .....	81
6.2.	Data Center Services High Level Requirements.....	82
6.3.	Data Center Services Environment .....	82
6.4.	Data Center Services Requirements, Roles and Responsibilities .....	83
6.5.	Application Server Services.....	84
6.6.	Infrastructure Services.....	95
6.7.	E-Mail Services .....	99
6.8.	Storage Services .....	103
6.9.	Managed Print Services.....	110
6.10.	Access Gateway Services.....	112
6.11.	Office Communications Services.....	113
<b>7.</b>	<b>Cross Functional Services.....</b>	<b>118</b>
7.1.	Cross Functional Services Overview .....	118
7.2.	Cross Functional Services High Level Requirements.....	118
7.3.	Security Management Services .....	119
7.4.	Billing Management Services .....	124
7.5.	Asset Management Services.....	126
7.6.	Contract Management Services.....	128
7.7.	Reporting Management Services .....	130
7.8.	Disaster Recovery Management Services .....	132
7.9.	Workflow Management Services .....	135
7.10.	Capacity and Performance Management Services.....	137
7.11.	Configurations Management Services .....	139
7.12.	Account Management Services .....	142
7.13.	Project Management Services .....	144
7.14.	Quality Assurance Services.....	146
7.15.	Transition Services .....	148
7.16.	Domain Names Management Services.....	149
<b>8.</b>	<b>Minimum Acceptable Service Levels.....</b>	<b>148</b>
<b>9.</b>	<b>Infrastructure Engineering Services.....</b>	<b>138</b>

## **1. Overview of Services**

### 1.1. Overview

This section describes the Services to be provided by the Contractor in various Service Frameworks, collectively also described herein as the Statement of Work (SOW). The objectives and requirements described in this Section 1 Overview of Services apply to all of the Service Frameworks unless specifically modified or augmented in a particular Service Framework. Capitalized terms used herein shall have the meaning assigned to them in Schedule A (Defined Terms) to the Agreement unless otherwise expressly defined in this Schedule.

### 1.2. High Level Requirements

1.2.1. Contractor shall provide IT and telecommunications services to the County with a high level of quality and performance that meet or exceed the Minimum Acceptable Service Levels (MASLs)

1.2.2. Contractor shall provide equal or better service on all Service Frameworks in performance, capacity, and functionality than prior to inception of this Agreement, except per the Agreement during Transition

1.2.3. Contractor shall improve the efficiency and effectiveness of County IT and telecommunications services over the life of the Agreement.

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

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

### 1.3. Service Environment

#### 1.3.1. Scope of Environment

All County IT and telecommunications services as described in this Schedule are within the scope of the Contractor's responsibilities, unless otherwise described in this Agreement.

#### 1.3.2. Hardware and Software

Contractor shall provide all hardware, software, tools and knowledge databases used in the delivery of Services for each Service Framework. Such assets will be provisioned, installed, managed, maintained, and supported by the Contractor. This includes, but is not limited to, the tools listed in Appendix 4.3.1

1.3.3. Facilities

1.3.3.1. County

All County Locations are within scope of the Agreement.

1.3.3.2. Contractor

All facilities (outside of County facilities) that are utilized by the Contractor to provide the Services will be provided, maintained, provisioned, and managed by the Contractor.

1.3.4. Personnel

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

1.3.5. Policies, Procedures and Standards

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

1.3.6. Agreement and Licenses

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

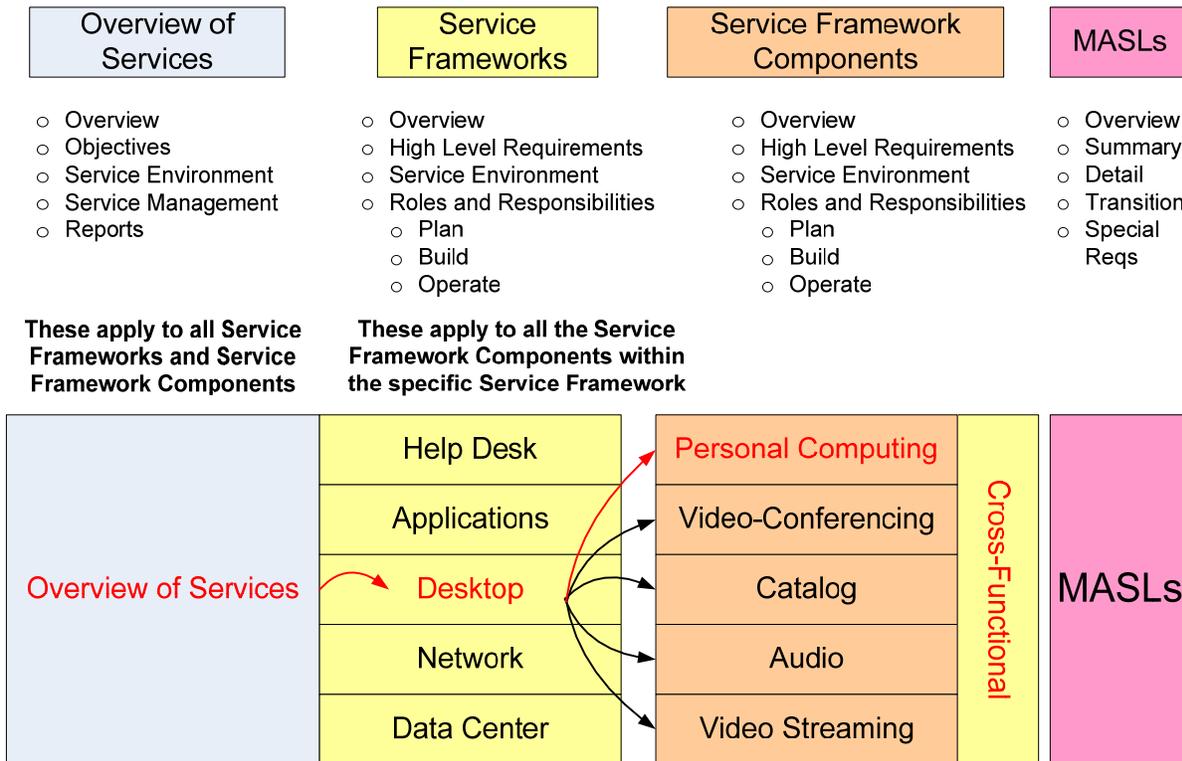
1.3.7. Required Language(s)

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

1.3.8. Service Requirements

**Schedule 4.3 – Operational Services**

Service requirements in this Section are described using the structure depicted below:



**Example: The Statement of Work objectives and requirements related to a Desktop PC are included in: 1) Overview of Services (which apply to the entire Statement of Work); 2) Desktop Services (which apply to all the components of the Desktop Services Framework); 3) Personal Computing (which apply to all end-user computing devices in the Desktop Services Framework); and 4) Cross-Functional Services (which apply to all Service Frameworks).**

The descriptions of Operational Services in this Schedule are based on the following hierarchy of objectives and requirements:

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

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

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

1.3.8.4 The Cross Functional Service Framework Components include requirements that apply to all of the other Service Frameworks and Service Framework Components

1.3.8.5 The MASL Section contains descriptions of minimum acceptable service level requirements that apply across the Service Frameworks

1.3.8.6 Within each section, tables describing Requirements, Roles, and Responsibilities are included. These tables are organized into the County’s Plan, Build, and Operate structure.

**2. Help Desk Services**

2.1. Help Desk Services Overview

This section pertains to the Help Desk Services framework. Help Desk Services consist of Plan, Build, and Operate centralized services to triage, process, track, and report on End-user requests for information and services.

2.2. Help Desk Services High Level Requirements

2.2.1 Contractor shall improve IT customer service and Problem resolution speed.

2.2.2 Contractor shall improve County efficiency and effectiveness by providing and utilizing knowledge databases and best practices in the areas of reporting, logging, tracking, resolving and reporting of IT Problems and Work Requests.

2.2.3 Contractor’s Help Desk Services will be part of a closed feedback loop process, so that the handling of issues will incorporate lessons learned, best practices, and appropriate solutions to improve economies, efficiencies, and performance.

2.2.4 Contractor shall ensure proficient and sufficiently skilled Help Desk support is available for new and emerging technologies as well as the County’s legacy technologies.

2.2.5 Contractor shall assist in the management and communication of modifications to the Services environment. All Install Move, Add and Remove (IMAR) requests will be facilitated by the Help Desk, including End-user notifications.

2.3 Help Desk Services Requirements, Roles and Responsibilities

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

<b>Help Desk Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit Help Desk solutions that best meet County business needs and service-level requirements	X	
2. Review and approve Help Desk solutions and service levels		X

**Schedule 4.3 – Operational Services**

<b>Help Desk Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
3. Perform operational planning for Help Desk capacity and performance purposes	X	
4. Perform analysis of County environment to identify the appropriate sets of skills, training, and experience needed by Help Desk staff	X	
5. Produce and submit operational policies and procedures including escalation	X	
6. Review and approve operational policies and procedures		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Develop and improve Help Desk scripts as appropriate to improve performance	X	
8. Provide all test services required to support Help Desk Services	X	
9. Produce and submit all test documentation to County	X	
10. Review and approve all test documentation		X
11. Provide all deployment services required to support Help Desk Services	X	
12. Produce and submit to County all deployment documentation	X	
13. Review and approve all deployment documentation		X
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
14. Manage all trouble tickets and services requests from inception to closure (e.g. recording, troubleshooting, escalating, coordinating, reporting, closing)	X	
15. Provide Help Desk Services, including provision, operation and maintenance of integrated Help Desk Systems (e.g. ACD, electronic workflow, problem management, self-help and self-heal, knowledge database, remote desktop control, procurement management, automated provisioning) necessary to document, track and manage trouble tickets and End-user service requests, inquiries and Problem notifications from inception to closure across Service Frameworks using cross functional processes	X	
16. Maintain and provide Help Desk operational policies and procedures in the Help Desk knowledge database	X	
17. Accept all incoming trouble calls and service requests via toll free telephone number, e-mail, fax, personal digital assistant (PDA) devices, IVR, or web access and direct appropriately	X	
18. Provide a single point of contact (SPOC) for, and coordinate all End-user requests for service	X	
19. Manage and track trouble tickets and service requests that involve multiple Service Frameworks and third parties (e.g. vendors, service providers, County staff) and collaborate with third parties to resolution and closure	X	
20. Provide third parties (e.g. vendors, service providers, County staff) access to the Help Desk Systems as required to support trouble ticket resolution and service requests (e.g. change management, asset management functions) per policies and procedures	X	
21. Utilize Help Desk Systems as required to resolve trouble tickets and perform service requests (e.g. change management, asset management functions) per policies and procedures	X	
22. Provide support for inquiries on the features, functions and usage of all portfolio applications and OIPC items in use at County	X	
23. Identify, escalate, and manage all End-user requests to closure	X	

**Schedule 4.3 – Operational Services**

<b>Help Desk Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
24. Support administration services such as creating, changing and deleting End-user Help Desk profiles	X	
25. Provide Help Desk call-in access via a toll free number	X	
26. Provide multiple alternative communications channels, including toll free voice number, web-based request, e-mail, and fax. In the case of voice communications, any IVR system must allow for immediate exit from the system and live communication with a Help Desk agent	X	
27. Provide Self-Help and Self Heal services for End-users that will include the following, at a minimum: <ul style="list-style-type: none"> <li>■ Password reset</li> <li>■ Request management and status checking</li> <li>■ Electronic bulletin board for posting of bulletins related to current service issues</li> </ul>	X	
28. Facilitate employee End-user account administration, activation, changes and terminations, including: password/account setup and reset, remote access connectivity, e-mail accounts, End-user IDs, password resets, remote paging devices, voicemail administration, telephone lines, secure ID cards, OIPC requests, etc.	X	
29. Prioritize calls to and from those County executives and Mission Critical End-users who have been identified by the County to Contractor	X	
30. Verify that all requests are resolved, per the End-user, prior to closure	X	
31. Diagnose problems using remote control tools and when possible implement remote corrective actions to resolve problems.	X	
32. Facilitate procurement management services including accurate and timely product procurement, from sourcing through order completion	X	
33. Track/manage/report Help Desk utilization	X	
34. Provide and maintain County escalation contact list(s)		X
35. Provide and maintain Contractor escalation contact list	X	
36. Provide and maintain Help Desk staff access to the County Directory	X	
37. Update County Directory data resulting from Help Desk services tasks	X	
38. Issue communications to provide status updates as required for planned and unplanned events	X	
39. Record and maintain an up-to-date System status message that may be selected when calling the Help Desk for assistance	X	
40. Provide End-user online access to all Work Requests	X	
41. Work with Contractor operational and technical staff, and County, to identify solutions that minimize the need to call the Help Desk (e.g., additional End-user training, self-help opportunities)	X	
42. Approve solutions that minimize the need to call the Help Desk		X
43. Ensure that response to End-user requests is based on County priority and impact	X	
44. Dispatch on-site technicians as necessary	X	
45. Categorize, prioritize and log all Break-Fix Tickets (e.g., inquiries/Problems/Work Requests)	X	
46. Monitor Break-Fix Tickets and escalate per policies and procedures until resolution and End-user satisfaction	X	

**Schedule 4.3 – Operational Services**

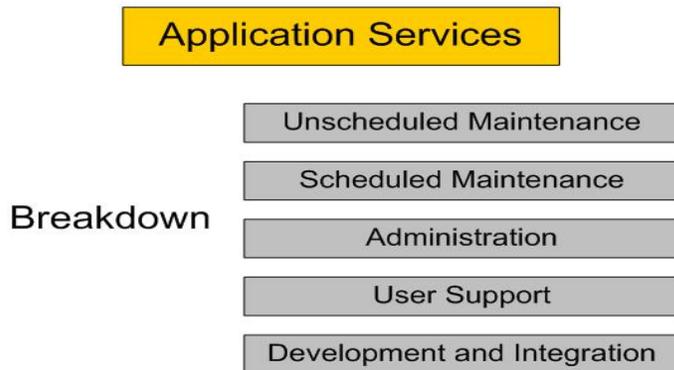
<b>Help Desk Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
47. Diagnose and troubleshoot problems at the Help Desk to resolve requests as quickly as possible	X	
48. Assist in enabling the enforcement of compliance to standards and the appropriate optimization at the desktop	X	
49. Utilize electronic workflow to coordinate and help perform End-user notifications related to IMAR requests including scheduling an appropriate, agreed time for the IMAR, to take place	X	
50. Maintain asset data and user profiles in the asset database through electronic workflow as a result from IMARs and related Cross Functional Services (e.g. change management, acquisition management, and asset management)	X	
51. Monitor and report on Help Desk statistics and trends (e.g., Work Request volumes and trends by types of End-users) for inclusion in the County of San Diego IT Management (CIM) Dashboard and MASL reporting	X	
52. Continuously review incident data to detect trends and to help manage high-priority incidents	X	
53. Report repetitive incidents, abnormal patterns of calls, and resolution recommendations to the County	X	
54. Produce and submit proposed changes to Help Desk processes, operations and procedures as services evolve	X	
55. Review and approve proposed changes to Help Desk processes, operations and procedures		X
56. Conduct periodic quality assurance audits of Help Desk documentation for accuracy and currency	X	
57. Submit all corrected documentation for County approval	X	
58. Conduct Help Desk End-user customer satisfaction surveys on a random sample of incidents (including both open incidents and incidents closed from the previous month) via an email/web based tool.	X	
59. Provide results of Help Desk End-user customer satisfaction surveys in the CIM Dashboard	X	

### 3. Application Services

#### 3.1. Application Services Overview

Application Services consist of activities associated with the development of new Applications, and maintenance/support of existing Portfolio Applications. The work categories are defined as follows: unscheduled maintenance, scheduled maintenance, administration, user support, and development and integration

#### Service Framework



#### 3.2. Application Services High Level Requirements

3.2.1 Contractor shall ensure all development and integration activities are aligned with the County IT Strategic Plan

3.2.2 Contractor will provide technology assistance and support to the County in planning and standard setting activities

3.2.3 Contractor will provide services in accordance with Information Technology Infrastructure Library (ITIL) standards and in accordance with CMMI standards to ensure practices result in predictable, repeatable, and successful results

#### 3.3. Application Services High Scope of the Environment

##### 3.3.1 Personnel

Contractor shall be responsible for staffing to meet the Applications labor categories as described in detail in Exhibit 16.1-4 to Schedule 16.1 to the Agreement Application Services Requirements, Roles and Responsibilities. Contractor will provide Application Services using the following staffing approach:

- Onsite presence at County Locations— A listing of Contractor Personnel to reside at various County Locations will be developed and included in the final Transition Plan.
- Local San Diego Center of Excellence (CoE)—The Contractor will have a CoE in the San Diego area. The CoE will house a majority of the Applications Team, including developers, additional functional resources, and applications management specialists.
- Remote locations in the continental US—Contractor will supplement the local resources with Subject Matter Experts (SMEs) in geographies outside the County.
- Contractor will provide a pool of personnel providing applications development and support across business groups

### 3.3.2 Unscheduled Maintenance

Unscheduled Maintenance shall include the repair of defects to enable Applications in production to provide the required functionality to meet the MASLs. Examples of Unscheduled Maintenance are:

- Non-latent defect - discovered/known (before Acceptance)
- Latent defect – discovered after Acceptance
- 3rd party defect
- No defect - defect ruled out

### 3.3.3 Scheduled Maintenance

Scheduled Maintenance shall include the following activities, which if not addressed proactively, could impact Applications in production, such as:

- Preventive maintenance/scheduled software updates
- Decommission/retire
- Application of System patches
- Proactive performance tuning
- Database administration

- Proactive archiving

Special testing for events, such as:

- Public holidays
- End of financial year
- End of calendar year
- Daylight savings time

#### 3.3.4 Administration

Administrative activities which include the following:

- User ID creation
- Table maintenance

#### 3.3.5 User Support

User support includes ancillary activities required for the proper operation of systems. The County's strategy is to decrease investment in this category of work. Tasks include:

- Meeting Attendance
- Planning/Analysis
- End-user Training
- Explanation of System Functionality

#### 3.3.6 Development & Integration

Development of new code and/or new functionality

- Integration and/or deployment of 3rd party software products
- Development of new database instances
- Development of interfaces

**Schedule 4.3 – Operational Services**

**3.4. Application Services Requirements, Roles and Responsibilities**

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

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Conduct periodic technical reviews	X	
2. Perform an annual portfolio analysis to identify and recommend Applications rationalization, consolidation, sun setting, etc.		X
3. Perform application portfolio optimization studies, including developing strategies such as “ERP Optimization” and “Application Rationalization” throughout the enterprise application environment to effectively capture operational savings and deliver productivity gains for the County of San Diego	X	
4. Assist in the annual portfolio analysis processes, including providing trend, technical, defect rate and cost information	X	
5. Produce and submit Project plans that include Project timelines, cost estimates, risk analysis, quality plans, and End-user training	X	
6. Review Project plans that include Project timelines, cost estimates, risk analysis, quality plans, and End-user training		X
7. Produce and submit vision & scope documents (conceptual plans) to define work to be performed	X	
8. Review and approve vision & scope documents		X
9. Define, refine, and prioritize business requirements		X
10. Assist in the development and integration, analysis and documentation of business requirements	X	
11. Perform business process reengineering activities as approved by the County	X	
12. Approve business requirements documents		X
13. Conduct County interviews, group workshops and surveys to determine technical, functional and End-user requirements for planning purposes	X	
14. Analyze Application software patches and releases to determine their applicability to the County environment, the level of effort necessary to adapt them to the County environment and any changes to hardware or other software changes necessary to support the patches and releases.	X	
15. Produce and submit functional business requirements documents, logical and physical data models and other requirements documentation for planning purposes	X	
16. Conduct value assessments of functional business requirements and generate an impact analysis, including affected systems, alternative high-level design scenarios, etc.	X	
17. Approve all functional requirements		X
18. Assist the County in the identification, evaluation and documentation of alternative Applications solutions to meet the County needs	X	
19. Conduct market analysis for commercial software solutions	X	
20. Approve software upgrade conversion requirements for COTS software		X

**Schedule 4.3 – Operational Services**

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
21. Recommend Application test plans (e.g., functional, volume, end-to-end, integration, stress, regression, system, and User Acceptance Test (UAT) if applicable) for planning purposes	X	
22. Produce and submit Application test plans	X	
23. Approve Application test plans		X
24. Produce and submit plans for Application integration	X	
25. Review and approve Application integration plan		X
26. Perform Project estimation using industry tools and methods to size Application Projects	X	
27. Produce and submit communication plans for rolling out changes to End-users	X	
28. Review and approve communication plans for rolling out changes to End-users		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
29. Provide project management services for Applications Services projects consistent with the Contractor’s standard methodology and Program Management Institute (PMI) processes.	X	
30. Produce and submit logical data model	X	
31. Approve logical data models		X
32. Produce and submit recommended technologies to support Applications	X	
33. Review and approve recommended technologies to support Applications		X
34. Conduct Site surveys for design efforts as required by requirements document	X	
35. Produce and submit detailed design documents based upon business and functional requirements and high-level design	X	
36. Review and approve detailed design documentation		X
37. Produce and submit technology designs that specify all program modules, data stores, interfaces, interface components and associated operations procedures for the Application	X	
38. Produce and submit technical requirements, logical and data models	X	
39. Review and approve technology designs, technical requirements and data models		X
40. Produce and submit test plans and test cases	X	
41. Approve test plans and test cases		X
42. Produce and submit implementation and deployment processes, Project schedules and staffing requirements to meet deployment and delivery requirements	X	
43. Review and approve implementation and deployment processes, schedules and deployment staffing levels		X
44. Produce and submit application software-related System specifications and documentation	X	
45. Produce and submit operational processing flows	X	
46. Produce and submit application software-related System installation, support, configuration and tuning manuals	X	
47. Produce and submit Application hardware and System software requirements documentation	X	

**Schedule 4.3 – Operational Services**

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
48. Produce and submit End-user manuals and other documentation	X	
49. Maintain, and provide County access to, physical and logical on-line libraries of all deliverables and documentation produced in the course of performing applications work (e.g., specifications, process flows, user manuals, operating manuals)	X	
50. Produce and submit standard operating procedures	X	
51. Produce and submit documentation for Applications on patches, updates and release notes	X	
52. Review and approve all Applications documentation submitted by the Contractor		X
53. Produce and submit a list of all Work Products to be developed during the Application build process prior to inception of the build process	X	
54. Review and approve the list of Work Products, including the level of review and approval for each Work Products		X
55. Establish overall programming and development and integration schedules	X	
56. Produce and submit overall programming and development and integration module delivery schedules for County Acceptance	X	
57. Approve overall programming and development and integration module delivery schedules		X
58. Perform all necessary programming, development, unit testing, scripting, configuring and customizing of Application modules as required to develop and implement the design plans and specifications	X	
59. Perform Application data base functions, including, but not limited to, development, monitoring and tuning	X	
60. Conduct and submit development and integration status reviews and provide written report on results to the County	X	
61. Conduct and submit development and integration status reviews with County and provide written report on results to the County	X	
62. Coordinate third party software vendors in the implementation of Application packages	X	
63. Integrate third party software solutions	X	
64. Assess results of Contractor development and integration reviews performed at the County's discretion		X
65. Produce and deliver prototypes	X	
66. Approve prototypes to ensure specifications are met		X
67. Produce and submit test plans, test cases, test data and perform all appropriate testing (e.g., unit testing, end-to-end testing, stress testing, regression testing)	X	
68. Approve all test plans		X
69. Produce and submit test environment and data where required by Project, including demonstration of requirements traceability to verify the requirements as specified in the requirements document have been satisfied	X	
70. Conduct and coordinate test activities	X	
71. Remediate Applications test results	X	
72. Review and approve test results		X

**Schedule 4.3 – Operational Services**

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
73. Facilitate and support User Acceptance Testing (UAT) establishing adequate test environment based on End-user Acceptance Criteria, preparing data to support test scenarios within modified System as well as managing the relationship with all interfaced Systems necessary to conduct testing, troubleshooting, supporting End-users to progress through scenarios, employing focused test teams using test scripts to perform important integration and Acceptance testing, simulating interfaces or working with integrated Systems to conduct end-to-end tests, support batch processing, exercise functionality, and report results, as requested by the County	X	
74. Manage and support software and test data in test environments	X	
75. Ensure testing results are in compliance with policies, procedures, plans, and test criteria and metrics (e.g., defect rates, progress against schedule)	X	
76. Notify Contractor in the event the County notices a discrepancy between the County’s requirements and the requirements document or Contractor deliverables		X
77. Define test-to-production turnover requirements and instructions for each Project or release	X	
78. Approve test-to-production turnover requirements and instructions		X
79. Produce and submit reports on results from test-to-production activities if applicable	X	
80. Review and approve reports on test-to-production results		X
81. Perform software support to migrate code from test to production as approved by the County	X	
82. Track migration status and notification	X	
83. Perform software support environment setup and decommissioning for new and changed environments	X	
84. Provide information on pertinent End-user policies and procedures		X
85. Provide software support for implementation and deployment of the County’s Application and platform environment in all County Sites as defined in the requirements document(s) or a Work Request	X	
86. Coordinate deployment and support activities with the County’s representatives as directed by the County	X	
87. Perform data migration from existing systems to new systems, by either electronic or manual methods	X	
88. Conduct post-implementation End-user Acceptance		X
89. Conduct post-implementation evaluation and review of new System implementation with County IT and End-user representatives to ensure effectiveness, usability and satisfaction	X	
90. Produce and submit Application and End-user documentation	X	
91. Produce and submit detailed “technical go-live” deployment plan	X	
92. Produce and submit “go/no-go” checklist	X	
93. Conduct the “go/no-go” meetings	X	
94. Review and approve production implementation “go/no-go” recommendation		X
95. Review and approve Application as “System of Record”		X
96. Produce and submit documentation to add to Applications Portfolio List	X	

**Schedule 4.3 – Operational Services**

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
97. Produce and submit End-user training plans	X	
98. Review and approve training plans		X
99. Produce and submit course material	X	
100. Review and approve course materials		X
101. Provide training materials	X	
102. Provide End-user training	X	
103. Produce and submit Help Desk scripts	X	
104. Review and approve Help Desk scripts		X
105. Produce and submit operations and administration procedures related to code migration	X	
106. Review and approve operations and administration procedures related to code migration		X
107. Conduct pre-installation site surveys, including validation of Site-specific functionality as defined in the Requirements Document(s)	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
108. Provide Application Unscheduled Maintenance	X	
109. Provide Application Scheduled Maintenance	X	
110. Provide Application User Support	X	
111. Provide Application Administration	X	
112. Deliver services using unified/consistent processes across all business groups and Applications to enhance quality, provide a common structure for service delivery and achieve maximum benefit from Application Services	X	
113. Produce and submit proposed production schedules for Applications	X	
114. Review and approve production schedules for Applications		X
115. Perform Application Software-related diagnostics	X	
116. Perform routine system management on Applications including patches and upgrades	X	
117. Produce and submit recommendations on operations and administration procedures related to code migration	X	
118. Review and approve recommended operations and administration procedures related to code migration		X
119. Maintain logical databases	X	
120. Define authorization requirements for End-users, roles, schemas, etc. and approve change requests		X
121. Perform ad hoc database restores	X	
122. Create/refresh development/test databases from production data	X	
123. Execute database creation, configuration, upgrades, patches and refresh	X	
124. Execute all database System level changes (initialization parameters)	X	
125. Execute all schema changes for all instances	X	

**Schedule 4.3 – Operational Services**

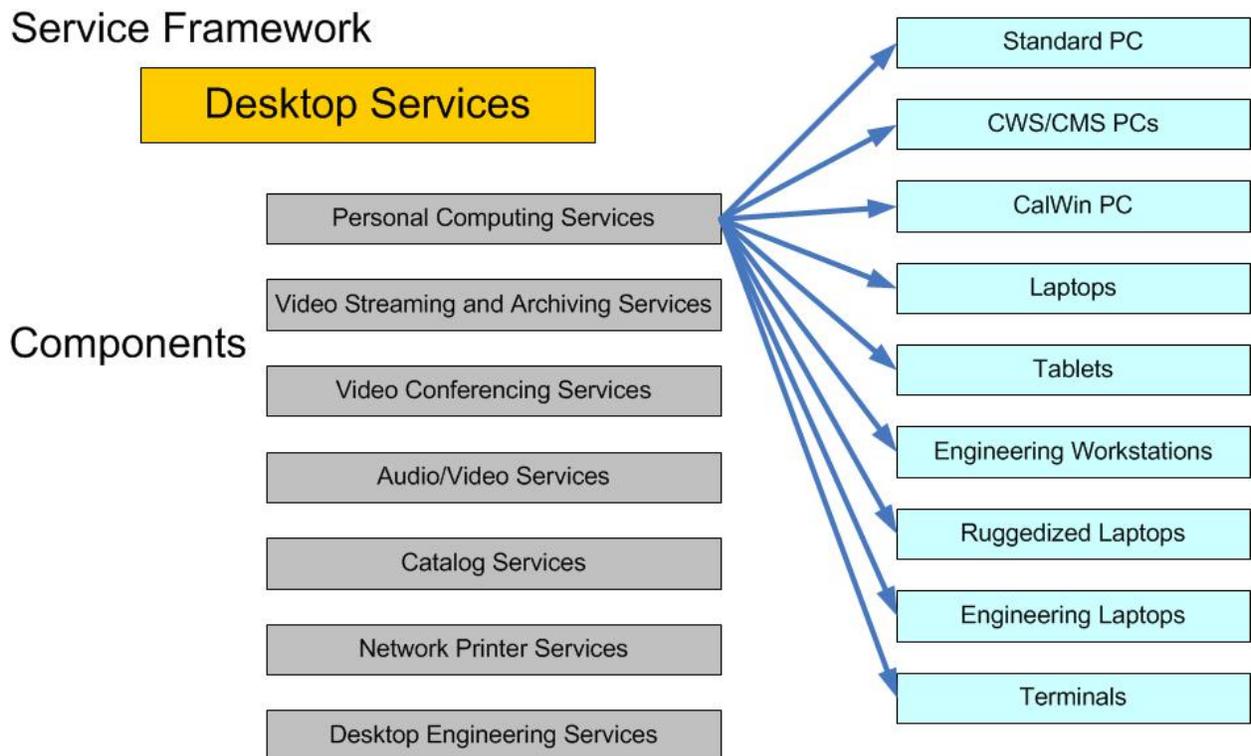
---

<b>Application Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
126.Perform database data definition activities for Applications per County requirements	X	
127.Maintain documentation for all database instance parameters and System settings	X	
128.Execute database data definitions and requirements	X	
129.Identify and resolve locking conflicts, latch contention, rollback requirements, etc. for all database instances	X	
130.Provide Application software-related technical assistance and subject matter expertise to County and third-party vendors.	X	
131.Provide data management support	X	
132.Produce and submit all Applications documentation	X	
133.Recommend database standards	X	
134.Implement County ad hoc reporting requirements	X	

#### 4. Desktop Services

##### 4.1. Desktop Services Overview

This section pertains to the Desktop Services Framework. Desktop Services consist of Plan, Build, and Operate services related to computing devices and peripherals (hardware and software) handled directly by End-users. Contractor shall provide centralized control of all Desktop Services, including Break-Fix and IMARs.



4.2. Desktop Services High Level Requirements

The following are the key high level requirements:

- 4.2.1. Contractor shall improve service and support levels
- 4.2.2. Contractor will provide technology assistance and support to the County in planning and standard-setting activities
- 4.2.3. Contractor shall improve End-user productivity
- 4.2.4. Contractor shall standardize hardware and software to the extent possible
- 4.2.5. Contractor shall improve asset management and control
- 4.2.6. Contractor shall improve total cost of ownership
- 4.2.7. Contractor shall support County’s business initiatives
- 4.2.8. Contractor shall provide IMAR services for the Desktop Services Framework
- 4.2.9. Contractor shall publish all Desktop Services asset standards on the County Intranet

4.3. Desktop Services Requirements, Roles and Responsibilities

The Contractor shall provide IMAR activities for the Desktop Services Framework. All IMAR activities require applicable updates to the Contractor’s Asset Management tracking system. IMAR activities are defined as:

4.3.1. Install

Contractor shall provide Install services as follows:

- 4.3.1.1. Order and deliver the Desktop Services Framework asset to the End-user workspace.
  - 4.3.1.2. Install the Desktop Services Framework asset, including configuration, setup, and network connection
  - 4.3.1.3. Perform all diagnostic testing to ensure Desktop Services Framework asset functionality
  - 4.3.1.4. Remove any boxes and/or packing materials
- 4.3.2. Move

Contractor shall perform Move services as follows:

4.3.2.1. Provide move services from within a Location or from Location to Location, for any Desktop Services Framework asset, which includes disconnecting, moving and reconnecting asset(s)

4.3.2.2. Perform all diagnostic testing to ensure Desktop Services asset functionality

4.3.3. Add

Contractor shall provide Add services as follows:

4.3.3.1. Provide upgrade or add hardware or software to deployed Desktop Services Framework assets

4.3.3.2. Provide upgrade or add features to requirements of the Work Request

4.3.3.3. Modify current configurations to deployed Desktop Services Framework assets to meet approved standards

4.3.4. Remove

Contractor shall perform Remove services as follows:

4.3.4.1. Provide Remove services for Desktop Services Framework assets that are being displaced due to Work Request, refresh or Break-Fix activity

4.3.5. Contractor shall provide update or upgrade software services as follows:

4.3.5.1. Use electronic tools for all networked attached desktop devices to deploy patches, applications, drivers, operating systems and any other upgrade

4.3.5.2. For non-network connected devices the Contractor will accomplish required updates and changes by providing the device user with a CD, DVD or an email containing the update or change. The Contractor will provide the device user with written instructions to execute the update or change. Phone assistance will be provided through the Team help desk, which will dispatch onsite support for additional assistance, as required.

4.3.6. Desktop Services Requirements, Roles and Responsibilities

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

**Schedule 4.3 – Operational Services**

<b>Desktop Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Recommend and submit hardware and software standards for Desktop Services assets	X	
2. Review and approve hardware and software standards for Desktop Services assets		X
3. Identify, recommend and submit Desktop Services solutions that best meet County’s business needs and expense/service level expectations	X	
4. Review and approve Desktop Services solutions and service levels		X
5. Perform operational planning for Desktop Services capacity and performance purposes	X	
6. Recommend and submit hardware and software deployment/management policies and procedures	X	
7. Review and approve hardware and software deployment/management policies and procedures		X
8. Recommend and submit hardware and software upgrades to Desktop Services assets	X	
9. Review and approve hardware and software upgrades to Desktop Services assets		X
10. Recommend and submit updates and patches plan to Desktop Services assets	X	
11. Review and approve updates and patches plan to Desktop Services assets		X
12. Update and provide to Contractor a list of County VIPs for use in MASL prioritization criteria		X
13. Recommend and submit MASL prioritization criteria based on the list of County VIPs	X	
14. Review and approve MASL prioritization criteria for County VIPs		X
15. Produce and submit preventive maintenance plans consistent with OEM practices. Plans shall include equipment model and manufacturer, frequency of PM, and specific actions to be taken such as cleaning, lubricating, adjusting, inspecting, running diagnostic tests, and replacing all parts and components defined by OEM as non-user replaceable or consumable necessary to keep the equipment functioning within the OEM specifications	X	
16. Review and approve preventive maintenance plans.		X
17. Produce and submit recommendations for “right sizing” printer to employee ratios	X	
18. Produce and submit tactical printer refresh strategy to determine the actual print need compared to the installed base	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
19. Provide all design and engineering required to deploy and support Desktop Services assets	X	
20. Produce and submit engineering documentation required to deploy and support Desktop Services assets	X	
21. Review and approve all engineering documentation required to deploy and support Desktop Services assets		X

**Schedule 4.3 – Operational Services**

<b>Desktop Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
22. Ensure Desktop Services solutions are fully integrated with the Help Desk Services Framework and asset management processes, including, but not limited to: <ul style="list-style-type: none"> <li>▪ A shared system and database</li> <li>▪ Direct electronic interfaces between the Help Desk agents and field service technicians</li> <li>▪ Integrated support processes involving desktop, data center, and network for remote server and telephone break-fix</li> </ul>	X	
23. Provide all test services required to support Desktop Services including providing a test laboratory that will develop and verify desktop images, as well as the support of desktop hardware and components evaluations and demonstrations	X	
24. Perform desktop software (e.g. applications, patch packages) and hardware functionality and product compatibility testing and development in the test laboratory environment using tools and procedures that are specially designed for this purpose (test to include: unit testing, system integration testing, LAN connectivity testing, load testing, and application interconnectivity testing)	X	
25. Develop and document test scripts	X	
26. Regularly monitor vendor websites and other communications for new application functionality, updates, and new software or hardware	X	
27. Build/Acquire updates and patches for Desktop Services assets	X	
28. Test updates and patches for Desktop Services assets	X	
29. Produce and submit deployment plan for updates and patches for Desktop Service assets	X	
30. Review and approve the deployment plan for updates and patches for Desktop Service assets		X
31. Produce and submit all build documentation	X	
32. Review and approve all build documentation		X
33. Produce and submit to County all test documentation	X	
34. Review and approve all test documentation		X
35. Produce and submit to County all deployment documentation for Desktop Services	X	
36. Review and approve all deployment documentation for Desktop Services		X
37. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices)	X	
38. Conduct deployment reviews and provide results to County	X	
39. Review and approve results of deployment reviews		X
40. Physically connect Desktop Services assets to the applicable wall jack	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
41. Provide technical support to End-Users for Break-Fix activities	X	
42. Ensure that desktop technicians have the tools necessary to improve problem resolution time	X	
43. Provide priority support for designated County Executives/VIPs	X	

**Schedule 4.3 – Operational Services**

---

<b>Desktop Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
44. Utilize auto discovery asset management tools to ensure most recent version of anti-virus software is installed	X	
45. Perform routine preventive maintenance according to the County approved preventative maintenance plans	X	
46. Regularly review asset data and failure trends and develop plans to review and proactively repair the equipment	X	
47. Perform predictive maintenance according to the County approved proactive repair plans	X	
48. Provide and maintain hardware and software documentation on desktops with the core or core + 1 images and provide others online through the online Web access	X	

#### 4.4. Personal Computing Services

##### 4.4.1. Personal Computing Services Overview

This section pertains to the Personal Computing Services component within the Desktop Services Framework. The Personal Computing Services component applies to all hardware and software needed to maintain and support Personal Computing Services assets. Personal Computing Services consist of activities associated with the Plan, Build and Operate of Standard PCs, CWS/CMS PCs, CalWin PCs, laptops, tablets, terminals and core software.

##### 4.4.2. Personal Computing Services High Level Requirements

4.4.2.1. Contractor shall provide standardization across the Personal Computing Services component for all hardware and software.

4.4.2.2. Contractor provided Personal Computing Services assets will be subject to refresh cycles as specified below

4.4.2.3. Contractor shall maintain currency of core software deployed within the Personal Computing Services component.

##### 4.4.3. Personal Computing Services Environment

###### 4.4.3.1. Scope of Environment to be Supported

The following sub-sections further describe and scope Personal Computing Services elements to be supported by Contractor and with which Contractor shall comply. For purposes of clarification, unless a Service is specifically limited or revised, all Services to be provided for “Retained Assets”, as set forth in this Section 4.4.3, will include all higher level requirements for 4.3 Operational Services, Section 4 Desktop Services, and Section 4.4 Personal Computing Services, as well as MASLs and Cross-Functional Requirements, per the Service Framework hierarchy of requirements described in Schedule 4.3, Section 1.3.8. The express inclusion of a Service does not imply the exclusion of other Services not identified.

###### 4.4.3.2. Hardware and Software

###### 4.4.3.2.1. Standard PCs

Standard PCs hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. For the first Contract Year, the standards will be those in effect with the Legacy Provider as of the date of Cutover for this Service Framework. The process to set Standard PCs hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Standard PC hardware will be refreshed within a 4-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 4-year cycle. Hardware and core software that meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

The Contractor will offer hard drive encryption services, under the Desktop Hard Drive Encryption Resource Unit, for those Standard PC assets the County has deemed require this service.

4.4.3.2.2. CWS/CMS PCs

The CWS/CMS PCs will comply with County core software standards. There will be no separate hardware standard setting process associated with CWS/CMS PCs. With the CWS/CMS PCs being Retained Assets, there will be no requirement for hardware refresh for this class of Personal Computing Services assets. The CWS/CMS PCs will be fully maintained and supported by the Contractor.

4.4.3.2.3. Department of Child Support Services (DCSS) PCs

DCSS PCs are Retained Assets owned by the State. After December 2007, the State CCSAS Business Partner, IBM Global Services, will provide DCSS PCs, including surplus PCs for operational readiness, and the standard for these PCs will be determined by CCSAS. The currently deployed PCs are all loaded with a DCSS core image, which is compatible with the current County core image. For the PCs to be provided the State CCSAS Business Partner, the CCSAS core image, which will be compatible with the then current County core image, will also be provided to Contractor by CCSAS and loaded on to the PCs by Contractor.

Contractor will perform hardware refreshes (for purposes of this Section, “hardware refresh” shall be defined as refresh labor only) for this class of Personal Computing Services assets: 1) in 2007 and 2) in 2011. Future refreshes will be performed every four years and in accordance with CCSAS refresh schedule. Each PC refresh cycle will include a monitor refresh, provided and determined by CCSAS. The refresh will be completed per the CCSAS refresh schedule and is not to exceed six calendar months. The PC refresh cycle will begin upon the receipt of the initial PC shipment from the State CCSAS Business Partner. In addition, Contractor will be responsible for IMARs, break-fix, and disposal for DCSS PCs in coordination with DCSS and the State.

4.4.3.2.4. DCSS Laptops

DCSS Laptops are Retained Assets owned by the State. After December 2007, the State CCSAS Business Partner, IBM Global Services, will provide DCSS Laptops, including surplus Laptops for operational readiness, and the standard for these Laptops will be determined by CCSAS. The currently deployed Laptops are all loaded with a DCSS core image, which is compatible with the current County core image. For the Laptops to be provided the State CCSAS Business Partner, the CCSAS core image, which will be compatible with the then current County core image, will also be provided to Contractor by CCSAS and loaded on to the Laptops by Contractor.

Contractor will perform two hardware refreshes (for purposes of this Section 4.4, “hardware refresh” shall be defined as refresh labor only) for this class of Personal Computing Services assets: 1) in 2007 and 2) in 2011. Each laptop refresh cycle will be completed per the CCSAS refresh schedule and is not to exceed six calendar months. The laptop refresh cycle will begin upon the receipt of the initial laptop shipment from the State CCSAS Business Partner In addition; Contractor will be responsible for IMARs, break-fix, and disposal for DCSS laptops in coordination with DCSS and the State.

.

4.4.3.2.5. CalWin PCs

The CalWin PCs will comply with County core software standards. There will be no separate hardware standard setting process associated with CalWin PCs. With the CalWin PCs being Retained Assets, there will be no requirement for hardware refresh for this class of Personal Computing Services assets. The CalWin PCs will be fully maintained and supported by the Contractor.

4.4.3.2.6. Laptops

Laptop hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. For the first Contract Year, the standards will be those in effect with the Legacy Provider as of the date of Cutover for this Service Framework. The process to set Laptop hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Laptop hardware will be refreshed within a 3-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 3-year cycle. Hardware and core software that meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

Laptop assets will be provisioned with hard drive encryption services.

4.4.3.2.7 Ultra-Portable Laptop

Ultra-Portable Laptop hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set Ultra-Portable Laptop hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Ultra-Portable Laptop hardware will be refreshed on a 3-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 3-year cycle. Hardware and core software that meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

Ultra-Portable Laptop assets will be provisioned with hard drive encryption services.

4.4.3.2.8 Engineering Workstations

Engineering Workstations are intended to provide additional computing power not available through the Standard PC resource unit. The process to set Engineering Workstation hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Engineering Workstations hardware will be refreshed within a 4-year cycle from initial installation as recorded in the Asset Management System. The asset refresh shall not be performed later than two months after the expiration of the 4-year cycle. Hardware and core software that

meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

#### 4.4.3.2.9 Ruggedized Laptops

Ruggedized Laptop hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set Ruggedized Laptop hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Ruggedized Laptop hardware will be refreshed within a 3-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 3-year cycle. Hardware and core software that meet current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process

Ruggedized Laptop assets will be provisioned with hard drive encryption services.

#### 4.4.3.2.10 Ruggedized Tablet

Ruggedized Tablet hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set Ruggedized Tablet hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year

The Ruggedized Tablet hardware will be refreshed on a 3-year cycle from initial installation as recorded in the Assets Management System.

Hardware and core software that meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

#### 4.4.3.2.11 Convertible Tablets

Convertible Tablet hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set Convertible Tablet hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

The Convertible Tablet hardware will be refreshed within a 3-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 3-year cycle. Hardware and core software that meet current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

Convertible Tablets assets will be provisioned with hard drive encryption services.

#### 4.4.3.2.12 Engineering Laptops

Engineering Laptop hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set Engineering Laptop hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year

The Engineering Laptop hardware will be refreshed within a 3-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 3-year cycle. Hardware and core software that meet the current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

Engineering Laptop assets will be provisioned with hard drive encryption services.

#### 4.4.3.2.13 Terminals

Terminal hardware standards and refresh are not applicable.

#### 4.4.3.2.14 Standard PC and Laptop Early Refresh Services

In response to a Standard PC or Laptop early refresh request by the County, via an IMAR, the Contractor will install approved replacement hardware, as requested by the County for currently installed Standard PC's or Laptops that have not yet reached the scheduled refresh date.

The Early Refresh Services only apply to situations where hardware Resource Unit is being replaced with a different hardware Resource Unit. Like for like refreshes are not provided under this service.

Hardware and Core Software that meet the current Contract Year standards for the replacement device, as called out in the Agreement, will be deployed as part of the refresh process, unless otherwise requested by the County.

#### 4.4.3.2.15 Core Software

Core software revisions will be reviewed annually by the County at least 60 days prior to start of new Contract Year and updates will go into effect at the start of each Contract Year. For the first Contract Year, the standards will be those in effect with the Legacy Provider as of the date of Cutover for this Service Framework. All assets in the Personal Computing Services Framework will maintain the same version of the core software throughout the given Contract Year. If updates are adopted, these updates will be placed onto all Personal Computing Services assets within a time frame set by County and agreed to by Contractor. At the County's request, Contractor shall recommend updates to the core software standards, for County's review and approval. Criteria for selection of a particular software package version upgrade will include that the software package has been field proven, necessary to the County for uninterrupted service to its customers, and poses no significant application remediation risks. The Contractor shall maintain the Core Software to within one version of the most current release (N-1). Any additions or deletions to the Core Software will be indicated in the Standards and Procedures Manual.

The Core Software as of January 2006 included:

- Microsoft Windows XP

- Microsoft Office 2003
- Microsoft Publisher
- Antivirus software
- WinZip
- Adobe Reader 7.x
- Internet Explorer 6.x
- Microsoft Windows Media Player
- Macromedia Shockwave/Flash Player
- Attachmate Extra Personal Client
- Roxio CD Creator Basic

#### 4.4.3.2.16 DCSS Core Software

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

- INFO Connect version 4.1

The DCSS Personal Computing Services asset refreshes in 2007 and 2011 will comply with the current Contract Year County Core Software standards (defined on an annual basis during the preceding Contract Year) with deference to the current CCSAS core software standard. In addition, CCSAS will provide the Operating System (OS) and Microsoft Office productivity software licenses.

#### 4.4.3.2.17 County Retained Assets

##### 4.4.3.2.17.1 Hardware and Software

The following are the County-retained Personal Computing Services Assets (“Retained Assets”) that are covered:

- County-retained Standard Desktops
- County-retained Laptops
- County-retained Convertible Tablets
- County-retained Engineering Laptops
- County-retained Standard Ruggedized Laptop

##### 4.4.3.2.17.2 Enrollment Requirements

The County shall enroll Retained Assets in accordance with the following requirements:

In order to be enrolled, the Retained Assets must be compliant with current Report 44 “Personal Computing Services Hardware Standards” or, for existing Retaining Assets, to previous version thereof within the preceding three-year period.

**4.4.3.2.17.3 Enrollment**

The County shall submit to Contractor an IMAR for the Retained Assets to be enrolled. Contractor will verify the requirements and enroll the Retained Assets.

**4.4.3.2.17.4 Services**

Contractor will provide the following services to the County enrolled Retained Assets:

Upon enrollment, Contractor will load an approved County standard image per the requirements of Report 43 “Personal Computing Services Core Software Standards”.

Every enrolled Retained Asset will be tagged with a Contractor’s asset tag in addition to the existing County property tag and will be tracked in Contractor’s asset management system.

Hardware support will be limited and provided only to enroll Retained Assets directly purchased through Contractor, or through Contractor authorized resellers, and accompanied by an extended hardware warranty. Hardware support will be limited to the services covered by such extended warranty. Retained Assets are excluded from the hardware refresh cycles.

**4.4.4 Personal Computing Services Requirements, Roles and Responsibilities**

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

<b>Personal Computing Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Recommend and submit Personal Computing assets hardware standards on a yearly basis	X	
2. Review and approve Personal Computing assets hardware standards		X

**Schedule 4.3 – Operational Services**

<b>Personal Computing Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
3. Recommend and submit core software standards for Personal Computing assets	X	
4. Review and approve core software standards for Personal Computing assets		X
5. Recommend and submit core software deployment/management policies and procedures	X	
6. Review and approve core software deployment/management policies and procedures		X
7. Produce and submit yearly Personal Computing asset refresh plan	X	
8. Review and approve yearly Personal Computing asset refresh plan		X
9. Recommend and submit Personal Computing software deployment/management policies and procedures	X	
10. Review and approve Personal Computing software deployment/ management policies and procedures		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Develop core software image for Personal Computing assets based on approved standards	X	
12. Test standard core software image for Personal Computing assets prior to deployment based on approved standards	X	
13. Review results of test and approve deployment for the core software image for Personal Computing assets		X
14. Deploy approved Personal Computing core software image.	X	
15. Provide staging services for Personal Computing assets at non-County Locations	X	
16. Deploy and manage desktop and laptop hardware and software (e.g., operating system, personal productivity and office automation software and services)	X	
17. Deploy software (e.g. patches, applications, drivers and operating systems) using a Contractor provided electronic software distribution tool	X	
18. Provide a rapid response team during software deployment for assisting affected End-users in the event a deployed package adversely affects End-users or any systems.	X	
19. Deploy, manage, communicate and report activities related to Personal Computing refresh	X	
20. Review and approve reports for Personal Computing refresh		X
21. Develop and provide training related to the implementation of new products and services	X	
22. Engineer the core software image and provide any and all version changes, upgrades, enhancements, and additions to the core software image, to ensure that the core software image will function properly on the desktop and the Applications Portfolio	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
23. Provide support, including break-fix, for all Personal Computing assets.	X	
24. Provide IMAR services	X	

**Schedule 4.3 – Operational Services**

<b>Personal Computing Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
25. Conduct data, End-user profile (e.g., favorites, bookmarks, MS Outlook profile) and Application migration that is necessary due to any Personal Computing refresh, IMAR or Break-Fix activity.	X	
26. Provide support for Personal Computing assets refresh	X	
27. Purchase, manage, and provide Personal Computing consumables (e.g., floppies, CDs) to the County’s employees		X
28. Purchase, manage, and provide Personal Computing consumables (e.g., floppies, CDs) to the employees of Contractor	X	
29. Provide core software updates, OIPC software installation and new software releases for Personal Computing assets	X	
30. Provide each End-user orientation on operational concepts of the new Personal Computing asset at time of deployment	X	
31. Provide and submit End-user tip sheets on such items as log on procedures, networked drives, system usage, core software, data storage and other practices that are essential to daily tasks	X	
32. Review and approve End-user tip sheets prior to deployment		X
33. Continually utilize automated asset management tools to identify unlicensed software on desktops and servers and to pinpoint desktop devices not running the most recent anti-virus software stipulated County standards and policies	X	
34. Provide software license and anti-virus software compliance reports to the County’s project manager and work to correct any non-compliance	X	
<b>END OF PAGE</b>		

4.5 Video Streaming and Archiving Services

4.5.1 Video Streaming and Archiving Services Overview

This section pertains to the Video Streaming and Archiving Services component within the Desktop Services Framework. The Video Streaming and Archiving Services component consists of the process of providing video data or content via a web page to the County Intranet or the external public and archiving such video data or content to be available for public viewing for one year. Video Streaming and Archiving Services consist of activities associated with the Plan, Build and Operate of the video streaming and Archiving service

4.5.2 Video Streaming and Archiving Services High Level Requirements

4.5.2.1 Contractor shall provide and maintain video streaming broadcast, of Board of Supervisors meetings, over the Internet to worldwide audiences and to the County Intranet.

4.5.2.2 Contractor shall deliver and distribute video streaming broadcasts of high quality video to all End-users.

4.5.2.3 Contractor shall provide and maintain video streaming capabilities across the County network.

4.5.2.4 Contractor shall archive video streamed broadcasts and store such archives for twelve months and provide a capability for public access, via the Internet, to and viewing of such archives.

4.5.2.5 Contractor shall provide a web-based service to collect feedback from citizens on specific items associated with upcoming Board of Supervisor’s meetings.

4.5.2.6 Contractor shall provide a custom web page for collecting the feedback and such web page will be activated by a link dropped on the County’s existing Board of Supervisors agenda page.

4.5.3 Video Streaming and Archiving Services Requirements, Roles and Responsibilities

**Schedule 4.3 – Operational Services**

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with Video Streaming and Archiving Services.

<b>Video Streaming and Archiving Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Provide support, including Break-Fix, for Video Streaming and Archiving Services	X	
2. Provide and maintain internet video and audio streaming broadcasts, including broadcasts of Board of Supervisors meetings.	X	
3. Provide archiving and public viewing and retrieval of broadcasts of Board of Supervisors meetings for twelve (12) months following the date of such meetings	X	
4. Provide broadcast feed of County of San Diego Board of Supervisors meetings to the Cox (or the applicable successor) cable television distribution network	X	

**4.6 Video Conferencing Services**

**4.6.1 Video Conferencing Services Overview**

Video Conferencing Services consist of the activities and functions of providing two-way video transmission between different entities within the County as well as outside of the County. These services may be used to enable closed-circuit video conference; point-to-point communications within County network connected sites; point-to-point to external State or Federal sites and; multi-point hosting of meetings. (Reference Schedule 16.1 Fees Section 15)

**4.6.2 Video Conferencing Services High Level Requirements**

4.6.2.1 Contractor shall provide a complete managed set of video conferencing system and services. Standards will be proposed annually by the Contractor and, once accepted by the County, published in the Standards and Procedures Manual.

4.6.2.2 Contractor shall wherever possible; refresh the County’s aging and obsolete video conferencing systems with new H323 standards based systems

4.6.2.3 Contractor shall provide infrastructure systems that monitors and maintains the QOS of the IP network (Gatekeeper) and supports secure off-net IP based video conferences (Border Controller).

4.6.2.4 Contractor shall provide Project Management for the installation of new systems. The installation interval is targeted to be 30 days or less, the actual installation period will be determined after a site review is conducted for that particular system. The Parties shall mutually agree, with the County requester, what services are considered beyond the scope of basic installation services.

4.6.2.5 Contractor shall provide basic installation which includes the assembly and placement of any furniture (roll-about cart), component or option provided as part of the new VTC system; along with the placement, connecting, configuration and testing of any electronics provided as part of the new VTC system and any other activities mutually agreed upon with the County.

4.6.2.6 Contractor shall provide point-to-point, multi-point and ISDN to IP video conferencing services to the County, both inside and outside the County's network.

4.6.2.7 Contractor shall provide and maintain the network security infrastructure to support external video conferences for all County departments.

4.6.2.8 Contractor shall provide video bridging service for County's use to facilitate ISDN to IP and multipoint video conferences. Contractor shall leverage the existing IMAR, Helpdesk and framework processes to manage and deliver all Video Conferencing Services.

4.6.2.9 Contractor shall provide single point of contact for break/fix call handling.

4.6.2.10 Contractor shall provide training to County department personnel for proper operation of hardware and software components & scheduling tool.

4.6.2.11 Contractor shall provide network access to new systems by trained and qualified video engineers and technicians to enable remote diagnostics and efficient triage of trouble reports.

4.6.2.12 Contractor shall provide access to manufacturer's customer service technical support center to assist County end users on equipment operation and any other questions they may have about the systems.

4.6.2.13 Contractor shall provide users access to the VTC 3<sup>rd</sup> Party Supplier's management system scheduling tool so that County end users can schedule their own video conferences.

**Schedule 4.3 – Operational Services**

4.6.2.14 Contractor shall provide software patches and version updates as recommended by equipment manufacturer limited to new systems provided under the VTC Resource Unit

4.6.2.15 of Video Conferencing Services assets.

4.6.2.16 Contractor shall provide parts and device warranty, repair and/or parts replacement of all components for systems of Video Conferencing Services.

4.6.2.17 Contractor shall comply with 4 business day service resolution [interval for service outage break/fix of systems (four 12 hour periods, Monday through Friday, 6AM to 6PM, excluding County holidays)].

4.6.2.18 Contractor shall provide a 5 year (1<sup>st</sup> month and month 61 of new systems) technology replacement/refresh of systems.

4.6.2.19 Contractor shall make recommendations to the County for new Video Conferencing Services strategy as new devices, infrastructures and protocols emerge.

4.6.2.20 Contractor shall provide a selection of Video Conferencing Services optional items via the OIPC Catalog.

**4.6.3 Video Conferencing Services Requirements, Roles and Responsibilities**

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

<b>Video Conferencing Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit plans for new, replacement and upgrades to Video Conferencing Services	X	
2. Produce and submit plans for infrastructure systems (Gatekeeper and Border Controller) and network capacities to support IP based VTC systems		
3. Review and approve plans for new, replacement and upgrades to Video Conferencing Services, infrastructure/network systems		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
4. Design and implement new, replacement or upgrades to Video Conferencing Services	X	
5. Design and implement infrastructure systems to support IP based VTC systems	X	
6. Design and implement network systems providing 512kbps to each IP based VTC system with Real-Time QOS provisioning	X	

**Schedule 4.3 – Operational Services**

<b>Video Conferencing Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
7. Review and approve design changes and implementation plans to Video Conferencing Services, infrastructure and network systems/circuits		X
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
8. Test and deploy approved changes to Video Conferencing Services including infrastructure systems and network services	X	
9. Develop and provide training related to the implementation of new products and services	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
10. Provide support, including Break-Fix, for new Video Conferencing Services, and limited Break-Fix for legacy Video Conferencing Systems (excluding parts replacement for legacy Video Conferencing Systems)	X	
11. Provide IMAR services	X	
12. Provide and support infrastructure services for point-to-point and multipoint video conferencing , Quality of Service and on-net/off-net video conferencing security	X	
13. Support Video Conferencing assets	X	

4.7 Audio/Video Services

4.7.1 Audio/Video Services Overview

Audio/Video Services consist of activities, equipment and services associated with the Plan, Build and Operate functions regarding Audio and Video assets including wiring and cabling. The County will request Audio/Video Services, when needed, via a Work Request.

4.7.2 Audio/Video Services High Level Requirements

4.7.2.1 Provide support for the existing Audio Services and upgrades upon request

4.7.2.2 Provide support for the existing Cable television cable plant and perform upgrades upon request.

4.7.3 Audio/Video Services Requirements, Roles and Responsibilities

All requests for service will be handled via a Work Request.

4.8 Catalog Services

4.8.1 Catalog Services Overview

Catalog Services consist of activities associated with the Plan, Build and Operate of the Optional Item Pricing Catalog (OIPC). The OIPC contains the hardware and software items that are approved for use within the County Desktop Services environment; consisting of distinct categories of goods and services available for purchase by the County. These categories are as follows:

Desktop Peripheral Hardware	Hardware physically connected to a Desktop asset, including, but not limited to, printers, scanners, keyboards, Blackberries, and monitor upgrades.
Standalone Hardware	Hardware that is not physically connected to a Desktop asset Including, but not limited to, videoconferencing optional equipment, audio/video equipment, and replacement parts.
Desktop Software	Classified in accordance with the Desktop Applications Directory (DAD). Includes acquisition, license management, engineering, deployment, rights management, and full maintenance of the software. DAD will be managed by the County, including adds, deletes, and updates of approved Applications on the list. Contract shall update and publish the OIPC on the County Intranet on a monthly basis.
Server-Hosted software	Server-hosted software not otherwise covered by a Resource Unit (i.e., Non-DAD Commercial Off-the-Shelf ("COTS") Software) as described in Section 16 of Schedule 16.1, Fees.
IT Training Courses	IT Training Courses (reference Section 4.8.3. of Schedule 4.3 and Section 12.1 of Schedule 16.1).

4.8.2 Catalog Services High Level Requirements

- 4.8.2.1 Maintain currency of items in the OIPC
- 4.8.2.2 The OIPC will be hosted and made available to County users on a proven table-driven catalog management system
- 4.8.2.3 Organize the OIPC to facilitate ordering and viewing for End-users
- 4.8.2.4 Publish the OIPC on an on-line County Portal, with online help functions, for viewing and ordering.

**Schedule 4.3 – Operational Services**

4.8.3 Catalog Services Requirements, Roles and Responsibilities

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

<b>Catalog Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Define, add, modify and delete hardware and software items in Optional Item Pricing Catalog (OIPC)		X
2. Produce and submit recommendations for updates to hardware and software items in the OIPC	X	
3. Review and approve updates to hardware and software items in the OIPC		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
4. Provide all engineering necessary to ensure functionality of all hardware and software items in the OIPC with Personal Computing assets	X	
5. Test all new and updated hardware and software items listed in the OIPC prior to deployment	X	
6. Develop and submit a deployment plan for any multi-End-User OIPC implementations	X	
7. Review and approve deployment plan for any multi-End-User OIPC implementations		X
8. Publish all new and updated items in the OIPC at the conclusion of the engineering activity	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Authorize items to be included in OIPC		X
10. Add or modify the DAD listed in the OIPC via a Work Request	X	
11. Maintain and support(as listed in the “Level of Support” section of the OIPC), including Break-Fix, all software and hardware in the OIPC	X	
12. Provide IMAR services for OIPC items	X	
13. Maintain and publish on a monthly basis the OIPC	X	
14. Provide web access and ordering capabilities for the OIPC to all County End-users	X	
15. Provide on-going OIPC user training	X	
16. Provide End-user orientation on operational concepts of new hardware or software installed via order from the OIPC	X	
17. Produce and submit IT training processes and procedures	X	
18. Review and approve IT training processes and procedures		X
19. Produce and submit recommendations for IT training courses	X	
20. Review and approve IT training courses		X
21. Design and deliver IT training courses as requested by a Work Request	X	
22. Provide IT training courses as requested	X	

*Schedule 4.3 – Operational Services*

---

<b>Catalog Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
23. Review new manufacturers' product posted offerings, verify the currency of the listed equipment, and maintain the accuracy of the OIPC	X	

#### 4.9 Network Printer Services

##### 4.9.1 Network Printer Services Overview

This section pertains to the Network Printer Services component within the Desktop Services Framework. The Network Printer Services component applies to all hardware and software needed to maintain and support networked Printer assets. Printers not attached or connected to the County network are excluded from this service. Network Printer Services consist of the activities associated with the Plan, Build and Operate of Monochrome Network Workgroup Printers – Standard Format, Monochrome Network Workgroup Printers – Large Format, Monochrome Network High Volume Workgroup Printers - Large Format, Color Network High Volume Workgroup Printers – Large Format and Color Network High Volume Workgroup Printers – Standard Format.

##### 4.9.2 Network Printer Services High Level Requirements

4.9.2.1 Contractor shall provide standardization across the Network Printer Services component for all hardware and software.

4.9.2.2 Network Printer hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year.

4.9.2.3 The Network Printer hardware will be refreshed within a 4-year cycle from initial installation as recorded in the Assets Management System. The asset refresh shall not be performed later than two months after the expiration of the 4- year cycle.

##### 4.9.3 Network Printer Services Scope of the Environment

###### 4.9.3.1 Hardware

4.9.3.1.1 Monochrome Network Workgroup Printer - Standard Format ( abbreviated as “MNWP”)

4.9.3.1.2 Monochrome Network Workgroup Printer – Large Format (11x17 capable)(abbreviated as “MNWP-LF”)

4.9.3.1.3 Monochrome Network High Volume Printer – Large Format (11x17 capable) (abbreviated as “MNWP-LF-H”)

4.9.3.1.4 Color Network Workgroup Printer – Large Format (abbreviated as “CNWP-LF”)

4.9.3.1.5 Color Network Workgroup Printer – Standard Format (abbreviated as “CNWP”)

The process to set Network Printer hardware standards will be based on recommendations made by the Contractor and provided in writing to the County. All printers models, meeting the Network Printer hardware requirements set forth in the section below, and complying with the requirements for setting hardware standards as contained in Schedule 4.3 of the Agreement, will be listed in the Report 44, Personal Computing Services Standards - Hardware Standards.

4.9.3.1.6 County purchased multi-function or specialized printer devices: Contractor will provide network connectivity and print queue installation for County purchased multi-function or specialized printer devices. Such devices will be reviewed with Contractor prior to selection.

**4.9.4 Network Printer Services Requirements, Roles and Responsibilities**

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

<b>Network Printer Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Recommend and submit Network Printer assets hardware standards on a yearly basis	X	
2. Review and approve Network Printer assets hardware standards		X
3. Produce and submit yearly Network Printer asset refresh plan	X	
4. Review and approve yearly Network Printer asset refresh plan		X
5. Recommend and submit Network Printer Services policies and procedures	X	
6. Review and approve Network Printer Services policies and procedures		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Provide staging services for Network Printer assets at non-County locations	X	
8. Deploy and manage Network Printer hardware and software (e.g., printer drivers)	X	
9. Deploy, manage, communicate and report activities related to Network Printer refresh	X	
10. Review and approve reports for Network Printer refresh		X

**Schedule 4.3 – Operational Services**

---

11. Identify the IT Coordinator for each deployed Network Printer prior to transition or deployment.	X	
12. Develop and provide training related to the implementation, use and operation of Network Printers	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
13 Provide support, including break-fix, for all Network Printer assets	X	
14 Provide Network Printer IMAR services	X	
15 Provide support for Network Printer assets refresh	X	
16 Provide printer driver updates	X	
17 Provide each IT Coordinator orientation on operational concepts of the new printer asset at time of deployment.	X	
18 Order and replace toner cartridges and paper from County office supply sources	X	

4.10 Desktop Engineering Service

4.10.1 Desktop Engineering Services Overview

Contractor will provide Desktop Engineering services as requested by the County in accordance with the Desktop Engineering Services stipulated in Schedule 16.1 Fees Section 18.

4.11 Mobile Device Management

4.11.1 Mobile Device Management Services Overview

This section pertains to the Mobile Device Management (MDM) Services component within the Desktop Services Framework. The Mobile Device Management Services are intended to allow faster and lower-cost adoption of productivity-enhancing iPhones, iPads Windows Phones/Tablets and Android devices; central control of County data (without impacting personal data); and enhanced security compliance across the enterprise. These services enable the Contractor to centrally manage and control all mobile devices, platforms and applications from a single unified console.

4.11.2 Mobile Device Management High Level Requirements

4.11.2.1 Contractor shall provide centralized, secure Mobile Device Management services for iOS, Android and Windows Phone devices (smart phones or media tablets).

4.11.2.2 Mobile Device Management Services shall include:

- Over-the-air (OTA) self-provisioning, policy setting on device and connection configuration, including the ability to set encryption, ActiveSync, VPN configuration and WiFi settings with audit verification to streamline activations and eliminate the need for IT involvement.
- All device policies will be based on County security and data policies developed into MDM platform format and recommended by the Contractor and approved by the County.
- Management and support of mobile devices management application includes MDM application updates, point releases and fixes as required; perform routine database maintenance, policy maintenance and backups; maintain the MDM configuration; troubleshoot MDM service-related issues; maintain certificates and password resets as required.
- Security enforcement to continuously audit all connected devices and quarantine or revoke service for unmanaged or compromised devices.
- Security protection to maintain control of County information and selectively wipe only County data and applications, or all data, from managed devices with audit of successful completion.
- Simplification of mobile application deployment with an enterprise-specific OTA catalog of mandatory, recommended and available applications, without requiring the use of a commercial Application Store such as GooglePlay or iTunes Store.
- ..

#### 4.11.3 Mobile Device Management Services Scope of the Environment

##### 4.11.3.1 Support Devices

The mobile devices supported on this service must be capable of being managed by the solution in place, which has been approved by the County/Contractor joint Enterprise Architecture Team. The devices must also meet the following minimum requirements:

- Devices must operate on these operating systems:
  - iOS: OS version 4.x or later
  - Android: OS version 2.6 or later
  - Windows 7: OS version 7.10 or later

- .

#### 4.11.3.2 “Bring Your Own Device” Program

The “Bring Your Own Device” or “BYOD” program allows County employees to enroll personal mobile devices under the Mobile Devices Management Service. County policy will dictate when “BYOD” is allowed. Devices under a BYOD program must comply with the requirements listed in Section 4.11.3.1 above..

#### 4.11.3.3 Devices excluded from the Mobile Devices Management Services

The following devices cannot be enrolled under the Mobile Devices Management Services:

- Devices that do not meet the criteria listed in Section 4.11.3.1 above
- Devices not authorized under the “Bring Your Own Device” Program
- Devices from County partners (such as Sheriff, DA, SDCERA)

#### 4.11.4 Mobile Device Management Services Roles and Responsibilities

##### 4.11.4.1 Authorize and Manage Mobile Users

Contractor shall manage mobile users by Active Directory (AD) group membership. This group membership will control end user’s ability to enroll in the Mobile Device Management service.

##### 4.11.4.2 Device Security Management

Contractor shall provide security management, including the general functionality described in this Resource Unit. The specific settings are defined by County policy as:

- Require passcode
- Wipe device after too many passcode attempts
- Restrict/Permit applications
- Restrict/Permit content
- Enforce application blacklist/whitelist

- Manage device configurations
- Manage Exchange and Active sync email configurations
- Ability to manage application sets and tie them to Active Directory is provided, but the labor for the addition, removal, modification or other actions for applications is not covered in this resource unit.
- In the event of lost or stolen assets, the asset will be wiped of all County data.

4.11.4.3 Mobile Device Application Store

The Contractor shall provide an Enterprise Mobile Device Application store. It can be used for application publishing to devices, through a push by user group. Labor for the creation or modification of applications for the Application Store shall be provided through Application Work Requests.

- The Application Store can be accessed from all supported devices.

4.11.4.4 Mobile Device Management - Requirements, Roles and Responsibilities

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

<b>Mobile Device Management Services: Plan, Build and Operate Requirements Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit Mobile Device Management solutions that best meet County business needs, security policies and service-level requirements	X	
2. Review and approve Mobile Device Management solutions		X
3. Perform and submit operational planning for Mobile Device Management capacity and performance purposes	X	
4. Review and approve operational planning for Mobile Device Management capacity and performance purposes		X
5. Design operational views and status for Ops Dashboard	X	
6. Review and approve operational views and statuses		X
7. Design operational reports per County Request	X	
8. Review and approve operational reports		X
9. Produce and submit Mobile Device Management operational policies and procedures including escalation	X	
10. Review and approve Mobile Device Management operational policies and procedures		X

**Schedule 4.3 – Operational Services**

<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Develop and improve Mobile Device Management build as appropriate to improve performance	X	
12. Provide all test services and produce documentation required to support Mobile Device Management	X	
13. Produce and submit all test documentation to County	X	
14. Review and approve all test documentation		X
15. Provide all deployment services required to support Mobile Device Management	X	
16. Produce and submit to County all Mobile Device Management deployment documentation	X	
17. Review and approve all Mobile Device Management deployment documentation		X
18. Produce and submit plans to apply Mobile Device Management application releases and patches as required	X	
19. Review and approve Mobile Device Management application releases and patches plans		X
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
20. Manage all trouble tickets and services requests from inception to closure (e.g. recording, troubleshooting, escalating, coordinating, reporting, closing)	X	
21. Produce and submit end user instructions on provisioning and configuration of mobile devices	X	
22. Review and approve end user instructions on provisioning and configuration of mobile devices		X
23. Provide over-the-air (OTA) self-provisioning and connection configuration	X	
24. Perform routine database maintenance and backups to maintain optimal performance of the Mobile Device Management Platform	X	
25. Maintain the Mobile Device Management Platform configuration per engineering build documents and County policy	X	
26. Maintain all Mobile Device Management certificates for the platform and the devices	X	
27. Perform all device specified services through the Mobile Device Management console (e.g. remote wipes and password resets)	X	
28. Provide continuous monitoring of all connected devices for security issues	X	
29. Quarantine or revoke service for any unmanaged or compromised mobile device	X	
30. Manage mobile devices through Active Directory group membership	X	
31. Manage County approved BYOD devices to specific applications authorized by the County	X	
32. Utilize Ops Dashboard to monitor system performance	X	
33. Provide operational reports as requested	X	
34. Manage Enterprise Application Store to add and delete mobile applications	X	

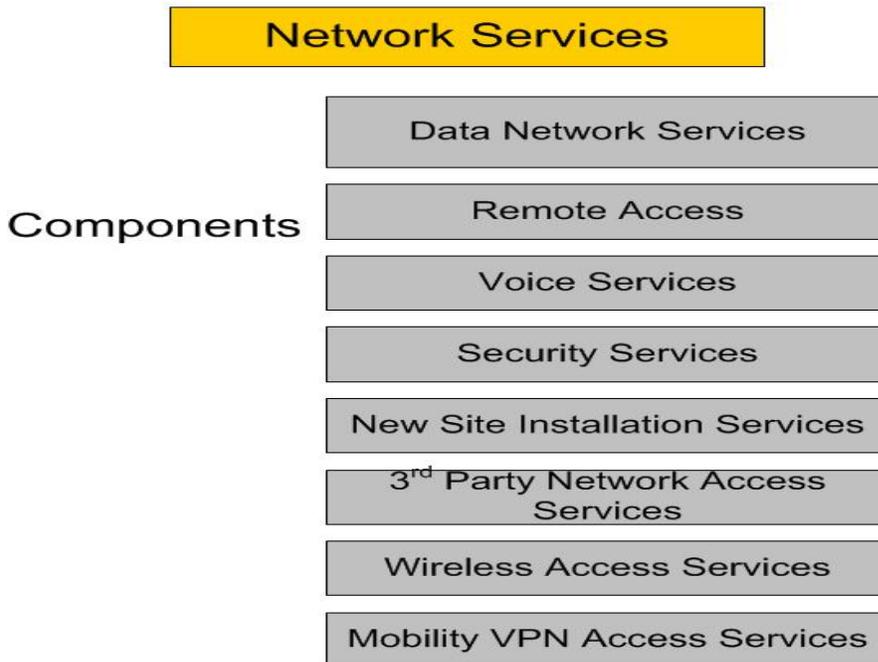
## 5 Network Services

### 5.1 Network Services Overview

5.1.1 Network Services include the assets and services associated with the electronic transport of data across the County infrastructure, and/or external third parties. The point of demarcation for Network Services with both Desktop Services and Data Center Services is the wall jack.

5.1.2 Network Services are comprised of the following components: Data Network; Remote Access; Voice Services; Security Services, New Site Installation Services, 3<sup>rd</sup> Party Network Access Services, Wireless Access Services and Mobility VPN Access Services. Activities included are the Plan, Build, and Operate of networked systems used for the transmission of information in voice, data, and/or video formats.

### Service Framework



### 5.2 Network Services High Level Requirements

5.2.1 Contractor shall provide a reliable, scalable, responsive and secure data communications network with connectivity to all Locations

5.2.2 Contractor shall meet County’s business needs for highly available, scalable, reliable, and secure voice communication services with features and functions that meet County business requirements

- 5.2.3 Contractor shall provide a core network architecture that is comprised of secure QoS managed Multi-Protocol Label Switching (MPLS) technology
- 5.2.4 Contractor shall implement a dedicated, secure, optical GigaMAN backbone
- 5.2.5 Contractor will provide technology assistance and support to the County in planning and standard-setting activities
- 5.2.6 Contractor shall maintain a secure network perimeter
- 5.2.7 Contractor shall provide secure network remote access to County users and authorized third parties
- 5.2.8 Contractor shall provide secure, reliable broadband internet connectivity that meets the County's bandwidth requirements
- 5.2.9 Contractor shall incorporate technology security improvements for business requirements without compromising the security, integrity, and performance of the County enterprise and its information resources
- 5.2.10 Contractor shall refresh and consolidate network assets to ensure operability and supportability
- 5.2.11 Contractor shall perform centralized management of network assets
- 5.2.12 Contractor shall provide additional network bandwidth as needed to meet County performance requirements, at no additional cost to the County
- 5.2.13 Ensure Sites have sufficient bandwidth to perform normal business functions
- 5.2.14 Ensure all network attached assets are operating at optimal and maximum performance
- 5.2.15 Ensure that all network assets related to network security are physically located in secure facilities off County premises, unless otherwise approved by the County
- 5.2.16 Interconnect all Sites to facilitate end-to-end business functions and allow network access to Shared Resources
- 5.2.17 Continuously manage and improve the network to meet the demands of the End-user and County business requirements including providing network bandwidth and technology upgrades as required

5.2.18 Continuously investigate technology that improves the overall network efficiencies, lowers overall network costs and improves End-user network satisfaction

5.2.19 Develop and implement a migration plan that spans the life of the Agreement and describes the future and current bandwidth requirements and maintains currency in network assets

### 5.3 Network Services Requirements, Roles and Responsibilities

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

**Schedule 4.3 – Operational Services**

<b>Network Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Collaborate with third party network carriers and vendors, and other industry leaders, on an initial and ongoing basis to develop and establish the most favorable, cost-effective strategic direction for voice technology for the County	X	
2. Produce and submit network architecture documentation	X	
3. Review and approve network architecture documentation		X
4. Produce and submit network asset refresh plan	X	
5. Review and approve network asset refresh plan		X
6. Produce and submit capacity and trending analysis for network infrastructure	X	
7. Review and approve capacity and trending analysis for network infrastructure		X
8. Produce and submit impact analyses and associated plans	X	
9. Review and approve impact analyses and associated plans		X
10. Produce and submit standards for network cable plant to include wiring standards, fiber standards, terminations, face plates, cable run, cable type.	X	
11. Review and approve standards for network cable plant to include wiring standards, fiber standards, terminations, face plates, cable run, cable type.		X
12. Produce and submit recommendations on maintaining the network cable plant to industry standard	X	
13. Review and approve recommendation on maintaining the network cable plant to industry standard		X
14. Produce and submit plans for Site additions or deletions upon request	X	
15. Review and approve plans for Site additions or deletions upon request		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
16. Design and implement network Architecture based on approved documentation	X	
17. Design, configure, deploy and report network assets based on the approved refresh plan	X	
18. Review and approve network asset refresh plan		X
19. Design and implement changes to the network infrastructure based on results of the capacity and trending analysis	X	
20. Design and implement changes to the network infrastructure based on impact analyses and associated plans	X	
21. Design and implement approved recommendations on maintaining the network cable plant to industry standard	X	
22. Implement network cable plant standards	X	
23. Design and implement network devices to meet County availability requirements (e.g. ensure that critical servers such as Domain Naming System (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory, e-mail, etc. have dual-attached network interface cards (NICs) to independent LAN switches and/or have back-up servers)	X	
24. Design and implement Site additions or deletions	X	

**Schedule 4.3 – Operational Services**

<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
24. Provide maintenance and support for all Network Services, including the cable plant, network hardware and circuits	X	
25. Perform proactive 24x7x365 network monitoring and maintenance functions for all framework components (e.g. voice systems, video systems, and data network transport) from County approved network operations centers (NOC)	X	
26. Provide centralized management of Network Services operations including Security	X	
27. Provide local (San Diego) 24x7x365 engineering technical support	X	
28. Implement and operate network management tools that automatically generate Help Desk trouble tickets in the event of network device failure	X	
29. Measure and benchmark the County’s server-to-desktop network performance using network performance tools	X	
30. Model and evaluate the effect that an introduction of a new application will have on the communications infrastructure and identify, quantify, and accommodate bandwidth requirements before production deployment of the application takes place	X	
31. Support and manage network cable plant to approved standards	X	
32. Provide updates to network Standards documentation as required	X	
33. Support site additions or deletions as requested	X	
34. Synchronize all network device time clocks using appropriate tools that meets county requirements (e.g. Network Time Protocol (NTP))	X	
35. Backup network device configurations	X	

**5.4 Data Network Services**

**5.4.1 Data Network Services Overview**

This section pertains to the Data Network Services component within the Network Services. The Data Network Services component applies to the physical network which encompasses the transmission (not processing) of information in various formats. Services provided within this component include, but are not limited to, network management, network capacity and performance monitoring, site to site connectivity, user to network connectivity, network engineering, Internet access and network refresh.

**5.4.2 Data Network Services High Level Requirements**

5.4.2.1 Contractor shall maintain currency on Data Network Services assets (Data Equipment)

5.4.2.2 Contractor shall propose a migration plan to update Data Network Services assets. The migration plan should update the Data Network Services assets

to supportable, current technology. The plan should be executed over a period of time, proposed by the Contractor, and should be a gradual, low-risk evolutionary process.

5.4.2.3 Contractor shall refresh Data Network assets on a 5 year refresh schedule, 20% per year, unless otherwise agreed to by the County in writing, and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of Data Network assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County (e.g., supervisor module in data network switch – a chassis upgrade may not be necessary).

. Contractor will defer refresh of the Data Network assets (i.e. LAN edge switches) for the periods; 1) September 30, 2011 through December 31, 2012 and; 2) January 1, 2014, unless otherwise directed by the County in writing. Contractor shall resume refresh as require in the Agreement commencing January 1, 2015. The Parties mutually agree to redirect funds that were originally allocated for the refresh of Data Network assets into the established Reinvestment Credit

The Parties agree that 40% of LAN Edge Switches deployed in the County environment as of January 2014 will not be refreshed by the end of the term of the Agreement. The specific equipment which will not be refreshed shall be designated by mutual agreement and shall be reflected in the Refresh plan submitted to the County on a yearly basis. At the resumption the refresh obligations, the refresh activity shall be equally distributed across all switch types.

The funds available and the use of in the Reinvestment Credits are defined in Schedule 16.1 Fees.

**5.4.3 Data Network Services - Requirements, Roles and Responsibilities**

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

<b>Data Network Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendation for Data Network Services architecture	X	
2. Review and approve recommendations for Data Network Services architecture		X
3. Produce and submit Data Network Services migration plan	X	
4. Review and approve Data Network Services migration plan		X

**Schedule 4.3 – Operational Services**

<b>Data Network Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
5. Produce and submit Data Network Services refresh plan on a yearly basis	X	
6. Review and approve Data Network Services refresh plan on a yearly basis		X
7. Identify, recommend and submit Data Network Services solutions that best meet County business needs and expense/service-level expectations	X	
8. Review and approve Data Network Services solutions and service levels		X
9. Perform and submit recommendations for Data Network Services capacity and performance policies and procedures	X	
10. Review and approve recommendations for Data Network Services capacity and performance policies and procedures		X
11. Produce and submit recommendations for Data Network Services migration to current technology	X	
12. Review and approve recommendations for Data Network Services migration to current technology		X
13. Produce and submit operational policies and procedures for monitoring and maintaining Data Network Services	X	
14. Review and approve operational policies and procedures for monitoring and maintaining Data Network Services		X
15. Produce and submit network provisioning policies and procedures	X	
16. Review and approve network provisioning policies and procedures		X
17. Produce and submit network administration policies and procedures	X	
18. Review and approve network administration policies and procedures		X
19. Produce and submit documentation of Data Network Services asset configuration files and IP addressing schemas	X	
20. Review and approve documentation of Data Network Services asset configuration files and IP addressing schemas		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
21. Produce and submit to County all design and engineering documentation to support Data Network Services	X	
22. Review and approve all design and engineering documentation for Data Network Services		X
23. Design, test and implement approved Data Network Services architecture	X	
24. Implement approved Data Network Services migration plan	X	
25. Deploy, manage, communicate and report on activities related to Data Network Services refresh	X	
26. Review and approve Data Network refresh report		X
27. Design and Implement Data Network Services capacity and performance policies and procedures	X	
28. Design, test and implement Data Network Services migration to current technology	X	
29. Implement operational policies and procedures for monitoring and maintaining Data Network Services	X	
30. Design and implement network provisioning policies and procedures	X	

**Schedule 4.3 – Operational Services**

<b>Data Network Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
31. Implement approved recommendations for Sites additions or deletions	X	
32. Implement approved network administration policies and procedures	X	
33. Order and expedite WAN circuits, assets and services	X	
34. Configure Data Network assets prior to installation	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
35. Provide support, including Break-Fix, for all Data Network Services assets	X	
36. Manage public carriers and other circuit providers to ensure delivery of WAN services	X	
37. Monitor Data Network Services to established baseline and thresholds	X	
38. Provide and support Data Network Services refresh	X	
39. Manage and support SNA network and assets	X	
40. Provide and support Data Network Services migration to new technology or architecture	X	
41. Produce and submit Data Network Services utilization, capacity and performance reports monthly	X	
42. Provide LAN/WAN connectivity to Locations and external entities	X	
43. Manage and support provisioning of new and upgraded Data Network Services assets	X	
44. Procure, provision and maintain all network components and circuits	X	
45. Provide support in accordance with approved network administration policies and procedures	X	
46. Perform day-to-day network operations and administration activities	X	
47. Maintain TCP/IP addressing schemes, router configurations, routing tables, VPN configurations, network addresses, MAC addresses, etc.	X	
48. Support legacy data networks and associated terminals, controllers and CSU/DSU, tied to current mainframe and midrange platforms	X	
49. Manage LAN infrastructure, including wiring, patch panels, jack configuration and documentation	X	
50. Implement measures for proactive monitoring and self-healing capabilities to limit network Break-Fix incidents	X	
51. Identify network Problems and Resolve in accordance with Break-Fix and Problem management services, polices, procedures and MASLs	X	
52. Perform and support physical (e.g., equipment) and logical (e.g., IP address change) IMAR associated with Sites for LAN/WAN and transport environments	X	
53. Manage the performance of public carriers (and other third parties) to meet defined schedules, Project plans, and performance	X	
54. Coordinate ordering, procurement and inventory management of network circuits from public carriers	X	

5.5 Remote Access Services

5.5.1 Remote Access Services Overview This section pertains to the Remote Access Services component within the Network Services. The Remote Access Services component applies to providing connection to internal County networked assets from outside the County network perimeters specifically for authorized End-users. Services provided within this component include, but are not limited to, VPN, Remote Access accounts, and dial-up access.

5.5.2 Remote Access Services High Level Requirements

5.5.2.1 Maintain a safe and secure session that allows authorized external and County End-users access to designated County network resources

5.5.2.2 Contractor shall refresh Remote Access Services assets on a 5 year refresh schedule, 20% per year, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of Remote Access Services assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County.

5.5.3 Remote Access Services Requirements, Roles and Responsibilities

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

<b>Remote Access Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for a consolidated Remote Access Services architecture	X	
2. Review and approve recommendations for Remote Access Services architecture		X
3. Produce and submit operational policies and procedures for Remote Access Services	X	
4. Review and approve operational policies and procedures for Remote Access Services		X
5. Produce and submit plans for updates and patches to Remote Access assets	X	
6. Review and approve plans for updates and patches to Remote Access assets		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Design, test and implement approved Remote Access Services	X	
8. Design and implement approved operational policies and procedures for Remote Access Services	X	

<b>Remote Access Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
9. Design, test and implement approved plans for updates and patches to Remote Access assets	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
10. Provide support, including break-fix, for all Remote Access Services assets	X	
11. Maintain, support and report on Remote Access Services	X	
12. Review and approve report on Remote Access Services		X
13. Maintain and support County Locations requiring Remote Access Services	X	
14. Maintain and support approved operational policies and procedures	X	

## 5.6 Voice Services

### 5.6.1 Voice Services Overview

This section pertains to the Voice Services component within the Network Services. The Voice Services component applies to hardware, software and circuits needed to operate the telecommunications within the County. Services provided within this component include, but are not limited to, single and multi-line voice services, single and multi-line, Voice over Internet Protocol (VoIP) services at County new Sites, Voice Mail, local dial plans, long distance plans, voice mail, Interactive Voice Services (Interactive Voice Response (IVR), Auto Attendants, Automated Call Distribution (ACD)) , analog jacks, telephone handsets and 4-1-1 operator services.

### 5.6.2 Voice Services High Level Requirements

5.6.2.1 Interconnect all Locations along a common voice network to facilitate end-to-end business functions, reduce toll calls and lower costs.

5.6.2.2 Contractor shall refresh Voice Services assets on a 5 year refresh schedule, 20% per year, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of Voice Services assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County (e.g., PBX network cards – a chassis upgrade may not be necessary).

5.6.2.3 The LAN/WAN supporting VoIP services will be provisioned to provide appropriate Quality of Service and 802.3af Power over Ethernet (POE). A single

cable drop as defined in Section 5.4 Data Network Services will be provided for joint use of the desktop and VoIP phones at locations where VoIP services are installed.

5.6.2.4 VoIP services will enable a Switched Ethernet connection for typical voice and data (desktop) services requiring connection to the County network.

5.6.2.5 Documentation that details operation and use of the operation and use of the VoIP telephone sets will be distributed to users of VoIP services.

5.6.2.6 VoIP hardware (voice station equipment) standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The process to set VoIP hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract year.

5.6.2.7 VoIP Services components include VoIP end user (Voice) station equipment and Voice Grade of Service elements consistent with Multi-Line and Single-Line Voice Jack Resource Units.

### 5.6.3 Voice Services Environment

#### Scope of the Environment to be Supported

The following further describe and scope Voice Services elements to be supported by Contractor and with which Contractor shall comply.

#### 5.6.3.1 Single-Line Voice Services

Single-Line Voice Services are all the hardware, software and services necessary to provide single-line phone services to End-users.

#### 5.6.3.2 Multi-Line Voice Services

Multi-Line Voice Services are all the hardware, software and services necessary to provide multi-line phone services to End-users.

#### 5.6.3.3 Single and Multi-Line VoIP Services

Single and Multi-Line VoIP services are all the hardware, software and services necessary to provide single and multi-line VoIP services to end-users.

#### 5.6.3.4 Voice Mail

Voice Mail is an option that can be added to Voices Services upon End-user request or a stand-alone option available to End-users without a phone. The ability to access Voice Mails from an End-user's e-mail inbox shall also be provided as an option for a number users selected by the County. The Voice Mail access shall be provided to the End-user through .WAV file sent as an attachment by e-mail to the End-user's e-mail inbox. The conversion of Voice Mail messages to text shall be also provided within the same email message.

#### 5.6.3.5 Analog Jack

The Analog Jack will be used to connect such hardware items as modems, or fax machines.

#### 5.6.3.6 Interactive Voice Services (IVS)

Interactive Voice Services (IVS) include services such as Interactive Voice Response (IVR), Auto Attendant and Automated Call Distribution (ACD) and is subject to the refresh requirements set forth for Voice Services. (Reference Schedule 16.1 Fees Section 14)

5.6.3.6.1 In instances where the County has obtained the development of an IVS either through the Contractor or a third party vendor and only requires ongoing support for the County owned IVS, Interactive Voice Services Support will be utilized. This would include, but is not limited to, circuitry, 24x7 maintenance support, circuit monitoring and fault detection, IMAR, Break/Fix support and Help Desk support, as set forth in Exhibit 16.1-1 and 16.1-2 and will be applicable regardless the complexity of the County owned IVS.

For County retained IVS systems obtained through a 3<sup>rd</sup> party, Contractor’s hardware and software support will be provided with ticket management through completion of break fix, although the actual support of the hardware and or software will be provided by the 3<sup>rd</sup> party supplier in accordance with the maintenance support requirements stipulated in the County 3<sup>rd</sup> party contract.

5.6.3.7 Telephone Handsets

Contractor shall provide telephone handsets as a function of Voice Services and will deploy telephone handsets corresponding to each type of active Voice Jack, and shall maintain (including replacement) such telephone handsets.

5.6.4 Voice Services Requirements, Roles and Responsibilities

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

<b>Voice Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for Voice Services solutions that best meets County business requirements	X	
2. Review and approve recommended Voice Services solutions that best meet County business requirements		X
3. Produce and submit operational plans for Voice Services capacity and performance management	X	
4. Review and approve operational plans for Voice Services capacity and performance policies and procedures		X
5. Produce and submit recommendations for Voice Services architecture	X	
6. Review and approve recommendations for Voice Services architecture		X
7. Produce and submit Voice Services refresh plan on a yearly basis	X	
8. Review and approve Voice Services refresh plan on a yearly basis		X

**Schedule 4.3 – Operational Services**

<b>Voice Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
9. Produce and submit recommendations for Voice Services migration to current technology	X	
10. Review and approve recommendations for Voice Services migration to current technology		X
11. Produce and submit operational policies and procedures for management and support of Voice Services	X	
12. Review and approve operational policies and procedures for management and support of Voice Services		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
13. Design, test and implement approved Voice Services solutions that best meet County business requirements	X	
14. Provide least cost routing (LCR) analysis and PBX technology that provides LCR (e.g. “tail end-hop off” LCR methodology)	X	
15. Implement approved operational plans for Voice Services capacity and performance management	X	
16. Design, test and implement Voice Services architecture		X
17. Deploy, manage, communicate and report on activities related to Voice Services refresh	X	
18. Review and approve Voice refresh report		X
19. Design, test and implement Voice Services migration to current technology	X	
20. Implement approved operational policies and procedures for management and support of Voice Services	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
21. Provide support, including Break-Fix, for all Voice Services assets	X	
22. Perform bandwidth management for Voice Services	X	
23. Support Voice Services refresh	X	
24. Support Voice network optimization and traffic engineering	X	
25. Provide competitive and economically favorable local and long distance rates	X	
26. Manage end-to-end internal and external phone connectivity including hardware and/or peripherals	X	
27. Manage the PBX systems to selectively eliminate central office caller ID call blocking, according to the authorized County personnel	X	
28. Manage PBX systems for class of service according to the authorized County key personnel	X	
29. Manage the PBX systems to provide least-cost routing and tail end hop off for outbound calls	X	
30. Manage interfaces between PBX network and public carriers	X	
31. Manage and support Interactive Voice Services	X	
32. Provide emergency 911 services to County phones	X	
33. Provide adaptive voice telecommunications services and equipment as required by laws affecting the support of the disabled	X	

**Schedule 4.3 – Operational Services**

<b>Voice Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
34. Manage and maintain private dial plan. An integrated numbering plan consistent with the County’s current dialing capabilities will be provided.	X	
35. Provide local and long distance voice services	X	
36. Support and manage long distance telephone calling	X	
37. Provide local and long distance usage monitoring and reporting	X	
38. Provide and support analog jacks for equipment such as modems, fax machines, or phones	X	
39. Provide Voicemail services	X	
40. Manage Voicemail security PBXs, voicemail systems, and other Voice Services assets	X	
41. Provide Voicemail usage monitoring and reporting	X	
42. Provide Voicemail storage capacity management	X	
43. Provide Voicemail retention management per County requirements and external regulations	X	
44. Perform Voicemail mailbox IMARs	X	
45. Maintain Voicemail mailboxes configurations by End-user	X	
46. Provide new Voicemail End-user training materials	X	
47. Provide access to voice messages through County’s email system.	X	
48. Provide directory services to the public through a mix of automated and live operators in order to meet call requirements	X	
49. Provide a secure and searchable online directory service with real time updates (e.g., global directory facility-GDF)	X	
50. Provide 4-1-1 operator services for the County which includes a directory of employees, employee locations, departments and telephone numbers	X	
51. Maintain a directory of County services for 4-1-1 operator services	X	
52. Provide 4-1-1 operator services for employee and public inquiries	X	
53. Update annually telephone numbers with SBC or successor Government pages	X	
54. Maintain and update an employee directory website with data from County Systems	X	
55. Maintain business process, systems, and information for phone book and directory assistance in accordance with County approved system design and business processes	X	
56. Provide teleconferencing services	X	
57. Provide on-demand and prescheduled teleconferences	X	
58. Provide proactive and reactive Voice Services fraud and security management and reporting	X	
59. Monitor and record all data, such as call rating tables, call usage detail and Move, Add, and Remove orders, generate cost allocation reports for local and long distance usage as well as completed Move, Add and Remove orders	X	
60. Provide itemized call detail records, including length of each call by telephone number and charge	X	

<b>Voice Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
61. Provide, maintain and support toll-free (on-net) calls between all County Locations	X	
62. Provide Casual Use Calling including collect calls, person-to-person calls, person-to-person collect calls, remote calls, operator assistance calls, 3rd party calls, dial one calls, dedicated calls and other miscellaneous calls	X	
63. Provide Conference Bridge Calls for calls placed to an audio and Web document sharing conference services that allow multiple people participation and is controlled by a unique access code.	X	
64. Provide Directory Assistance Calls for calls placed to obtain a listed telephone directory number	X	
65. Provide Pay Phones located at County facilities for the public’s convenience, which are required by statute.	X	

## 5.7 Security Services

### 5.7.1 Security Services Overview

The Security Services component of Network Services includes the hardware, software, and services provided to maintain network security, including:

- Protection from unauthorized devices, software or users
- Protection from unauthorized access to, or use of, the network and networked assets
- Firewall services
- Intrusion detection and reporting
- Security monitoring
- Security architecture services
- Data protection
- Prevention of malicious code entry into the network.

### 5.7.2 Security Services High Level Requirements

5.7.2.1 Develop and maintain flexible security architecture

5.7.2.2 Provide protection from unauthorized use of, or access to, the County’s network and networked assets.

5.7.2.3 Protect all data residing on the network from intrusion, destruction or compromise.

5.7.2.4 Contractor shall refresh Security Services assets on a 5 year refresh schedule, 20% per year and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of Security Services assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County.

### 5.7.3 Security Services Environment

The following further describes and scope of Security Services elements to be supported by Contractor and with which Contractor shall comply.

#### 5.7.3.1 Intra-County and Public Network Access Security Services

This includes all the Security Services associated with network usage and services for County end-users and the public, including Security Services for:

5.7.3.1.1 County data jacks

5.7.3.1.2 County voice jacks

5.7.3.1.3 Remote access

5.7.3.1.4 Access to and from the County network through the Internet

5.7.4 Security Services Requirements, Roles and Responsibilities

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

<b>Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for Security architecture	X	
2. Review and approve recommendations for Security architecture		X
3. Produce and submit plans for monitoring and managing access to the County Intranet	X	
4. Review and approve plans for monitoring and managing access to the County Intranet		X
5. Produce and submit plans that provide security to physical and logical devices connected to the network	X	
6. Review and approve plans to include the provision and support of methods that provide security to physical and logical devices connected to the network		X
7. Produce and submit recommendations on firewall policies that comply with County policy	X	
8. Review, approve and identify firewall policies that comply with County policy		X
9. Produce and submit recommendation of Security Services assets refresh or upgrade plan on a yearly basis	X	
10. Review and approve recommendations on Security Services assets refresh or upgrade plan		X
11. Produce and submit recommendations for improved network security	X	
12. Review and approve recommendations for improved network security		X
13. Produce and submit recommendation of policies for security vulnerability & penetration testing	X	
14. Review and approve policies for security vulnerability & penetration testing		X
15. Produce and submit plans for Security Services asset updates or patches	X	
16. Review and approve plans for Security Services asset updates or patches		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
17. Design, test and implement approved Security architecture	X	
18. Design and implement monitoring and managing access plans as approved	X	
19. Design, test and implement plans to secure network attached devices	X	
20. Design, test and implement approved firewall policies	X	
21. Design, test, implement and report Security Services assets refresh or upgrade	X	
22. Review and approve reports for Security Services assets refresh or upgrade		
23. Design and implement approved recommendations for improving network security	X	
24. Design and implement approved policies for security vulnerability & penetration testing	X	

**Schedule 4.3 – Operational Services**

<b>Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
25. Design, test and implement updates or patches approved for Security Services assets	X	
26. Enable technologies that use a centralized authentication database for remote County employees, contractors and agents using VPN and will deploy new systems capable of interfacing with single-sign-on authentication services	X	
27. Deploy a Security Information Management System (SIMS) for aggregation and centralization of incident alerts and correlation and provide SIMS information to the County through online access	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
28. Provide support, including break-fix, for all Security Services assets	X	
29. Provide 24x7x365 security monitoring services including a Security Operations Center (SOC), IDS/IPS infrastructure and intranet/Internet firewalls	X	
30. Provide Services in conformance to firewall policies and requirements	X	
31. Provide reporting on security testing results	X	
32. Provide initial review of security Break-Fix incidents and the determination if escalation, including to County Information Security, is warranted	X	
33. Provide standardized End-user operations and capabilities and also custom reports regardless of the End-user’s location and/or department	X	
34. Identify and remove from the network any malicious-code (malcode) infected System	X	
35. Identify and provide countermeasures for malcode attacks (i.e., both prevention and remediation)	X	
36. Block unauthorized party access and provide notification of unauthorized access attempts	X	
37. Encrypt (and prioritize) all County traffic that uses public MPLS network transport facilities (such as OPT-E-MAN or DSL) through the engineering and implementation of generic routing encapsulation (GRE) VPN tunnels (e.g. 256-bit Advanced Encryption Standard (AES) key)	X	
38. Provide technical expertise for security audits	X	
39. Collect all logs and review all Break-Fixes reported by all other security services (e.g. NIPS, HIPS, penetration testing, and firewall).	X	
40. Maintain log files in accordance with County policies and MASLs	X	
41. Provide security reporting	X	
42. Provide fraud prevention, detection and reporting	X	
43. Provide, control, monitor, and maintain security encryption interface at the data network level	X	
44. Provide security devices on supported PBXs, voicemail systems, and other appropriate adjunct remote administration ports	X	
45. Implement security violation notification. This function notifies a designated station/End-user/administrator when a hacker attempts to breach System management	X	

Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities		
Plan Requirements, Roles and Responsibilities	Contractor	County
46. Conduct security perimeter vulnerability assessments and annual penetration testing	X	

5.8 New Site Installation Services

5.8.1 New Site Installation Services Overview

This section pertains to the New Site Installation Services component within the Network Services Framework. The New Site Installation Services component applies to the Plan and Build tasks needed for a new, networked County Location.

Services provided within this component are one-time activities that include, but are not limited to, setup of MDF/IDF, installation of network Equipment (note: the network equipment itself is included in the Data Network and Voice Services components), installation of Voice and Data Network cable plant (including trenching as required), installation of WAN circuit(s), and all Planning and Engineering required to ensure site functionality.

5.8.2 New Site Installation Services High Level Requirements

5.8.2.1 Install new County Locations using the following Site Type definitions:

5.8.2.2 Type I – are defined by having either more than 1,000 voice jack Resource Units or more than 1,000 data jack Resource Units

5.8.2.3 Type II – are defined by having either between 301 and 1,000 voice jack Resource Units or more than 300 data jack Resource Units

5.8.2.4 Type III – are defined by having either between 11 and 300 voice jack Resource Units or more than 10 data jack Resource Units and are typically extensions of Type II Sites

5.8.2.5 Type IV – are defined by having between 1 and 10 voice jack Resource Units and 3 or more data jack Resource Units.

5.8.2.6 Type V – are defined by having between three (3) and ten (10) data jack Resource Units.

5.8.2.7 Type VI - are defined by having either ten (10) or fewer voice jack Resource Units or two (2) or fewer data jack Resource Units

**Schedule 4.3 – Operational Services**

5.8.2.8 Establish and maintain a predictable cost and methodology to install a new networked County Location

5.8.2.9 Install sufficient data and voice ports that meet standards for network cable plant and match the number of projected users for the site.

**5.8.3 New Site Installation Services Requirements, Roles and Responsibilities**

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with New Site Installation Services.

<b>New Site Installation Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Submit Work Request to initiate New Site Installation indicating Site Type		X
2. Produce and submit plans for New Site Installation	X	
3. Review and approve plans for New Site Installation		X
4. Produce and submit policies and procedures for New Site Installation	X	
5. Review and approve policies and procedures for New Site Installation		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
6. Design and implement New Site Installation	X	
7. Implement County approved policies and procedures for New Site Installation	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
8. Support New Site Installation policies and procedures	X	

**5.9 3<sup>rd</sup> Party Network Access Services**

**5.9.1 3<sup>rd</sup> Party Network Access Services Overview**

This section pertains to the 3<sup>rd</sup> Party network access Services component within the Network Services. The 3<sup>rd</sup> Party network access Services component applies to security services and network bandwidth needed by an authorized 3<sup>rd</sup> party entity to gain access to the County network. Services provided within this component include, but are not limited to, protection from unauthorized network access, firewall services, intrusion detection and reporting, security monitoring, data protection, network management, network capacity and performance monitoring, and 3<sup>rd</sup> party network to County network connectivity.

**5.9.2 3<sup>rd</sup> Party Network Access Services High Level Requirements**

5.9.2.1 Establish and maintain 3<sup>rd</sup> Party network access to County data network

5.9.2.2 Contractor shall refresh 3<sup>rd</sup> Party network assets (as defined in Section 5.9.1 above) on a 5 year refresh schedule, 20% per year, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of 3<sup>rd</sup> Party (County) network assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County.

5.9.3 3<sup>rd</sup> Party Network Access Services Environment

5.9.3.1 Scope of the Environment to be Supported

The following further describe and scope 3<sup>rd</sup> Party network access Services elements to be supported by Contractor and with which Contractor shall comply.

- Security Services

Security Services include all the hardware, software, and services provide to ensure secure and authorized access to the County network and networked assets via private network interconnections into the County network (e.g., for the Sheriff’s network, District Attorney’s network).

- Network Services

Network Services include all the hardware, software, and services needed by a 3<sup>rd</sup> party to access County network assets. This will be made up of three (3) categories of private network circuits or connections from a 3<sup>rd</sup> Party to the County, IPSEC Tunnels and Virtual Access. The circuit connecting to the County is the responsibility of the 3<sup>rd</sup> Party.

1. Private Circuit/Connection

Category 1 – any circuit or connection less than T1 speed (1.544mbps)

Category 2 – any circuit or connection equal to T1 speed

Category 3 – any circuit or connection greater than T1 speed

2. IPSEC Tunnels Connection

IPSEC Tunnel 5Mbps

IPSEC Tunnel 10Mbps

3. Virtual Access Connection

Virtual Access 1Mbps

Virtual Access 2Mbps

Virtual Access 3Mbps

Virtual Access 4Mbps

Virtual Access 5Mbps

Virtual Access 6-10Mbps

5.9.4 3<sup>rd</sup> Party Network Access Services Requirements, Roles and Responsibilities

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with 3<sup>rd</sup> Party Network Access Services.

<b>3<sup>rd</sup> Party Network Access Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for 3 <sup>rd</sup> Party network access architecture	X	
2. Review and approve recommendations for 3 <sup>rd</sup> Party network access architecture		X
3. Produce and submit plans for monitoring and managing access to the County network from 3 <sup>rd</sup> Parties entities	X	
4. Review and approve plans for monitoring and managing access to the County network from 3 <sup>rd</sup> Parties entities		X
5. Produce and submit recommendations on firewall policies that comply with County policy	X	
6. Review and approve firewall policies		X
7. Produce and submit recommendation of 3 <sup>rd</sup> Party network access Services assets refresh or upgrade plan on a yearly basis	X	
8. Review and approve recommendations on 3 <sup>rd</sup> Party network access Services assets refresh or upgrade plan		X
9. Produce and submit plans for 3 <sup>rd</sup> Party network access Services asset updates or patches	X	
10. Review and approve plans for 3 <sup>rd</sup> Party network access Services asset updates or patches		X

**Schedule 4.3 – Operational Services**

<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Design, test and implement approved 3 <sup>rd</sup> Party network access architecture	X	
12. Design and implement monitoring and managing access plans as approved	X	
13. Design, test and implement approved firewall policies	X	
14. Design, test, implement and report 3 <sup>rd</sup> Party network access Services assets refresh or upgrade	X	
15. Review and approve reports for 3 <sup>rd</sup> Party network access Services assets refresh or upgrade		X
16. Design, test and implement updates or patches approved for 3 <sup>rd</sup> Party network access Services assets	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
17. Provide support, including break-fix, for all 3 <sup>rd</sup> Party network access Services assets	X	
18. Provide Services in conformance to firewall policies and requirements	X	
19. Support 3 <sup>rd</sup> Party network access Services refresh	X	
20. Manage network interfaces between the County and 3 <sup>rd</sup> Parties	X	
21. Produce and submit network utilization, capacity and performance reports	X	
22. Provide initial review of security Break-Fix incidents and the determination if escalation, including to County Information Security, is warranted	X	
23. Provide standardized End-user operations and capabilities and also custom reports regardless of the End-user’s location and/or department	X	
24. Identify and remove from the network any malicious-code (malcode) infected System	X	
25. Identify and provide countermeasures for malcode attacks (i.e., both prevention and remediation)	X	
26. Collect all logs and review all Break-Fixes reported by all other security services (e.g. NIPS, HIPS, penetration testing, and firewall).	X	
27. Maintain log files in accordance with County policies and MASLs	X	
28. Provide security reporting	X	
29. Provide fraud prevention, detection and reporting	X	

5.10 Wireless Access Services

5.10.1 Wireless Access Services Overview

This section pertains to the Wireless Access Services component within the Network Services Framework. The Wireless Access Services component applies to the 802.11x wireless access points located at County Sites. The Wireless Access Points can allow multiple, secure and authorized wireless connections into the County network.

**Schedule 4.3 – Operational Services**

Services provided within this component include, but are not limited to, network management, network capacity and performance monitoring, wireless network security, network engineering, and asset refresh.

**5.10.2 Wireless Access Services High Level Requirements**

5.10.2.1 Contractor shall maintain currency on Wireless Access Services assets

5.10.2.2 Contractor shall ensure that all devices that attached to the Wireless Access Services are valid and authorized

5.10.2.3 Contractor shall ensure that the Wireless Access Services network is secure

5.10.2.4 Contractor shall refresh Wireless Access Services assets based on a five (5) year refresh cycle and the asset’s installation date

5.10.2.5 Contractor shall make available two types of Wireless Access Points interior mounted and exterior mounted.

**5.10.3 Wireless Access Services Requirements, Roles and Responsibilities**

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

<b>Wireless Access Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendation for Wireless Access Services architecture	X	
2. Review and approve Wireless Access Services architecture		X
3. Produce and submit Wireless Access Services refresh plan on a yearly basis	X	
4. Review and approve Wireless Access Services refresh plan on a yearly basis		X
5. Produce and submit Wireless Access Services policies and procedures	X	
6. Review and approve Wireless Access Services policies and procedures		X
7. Produce and submit Wireless Access Services security architecture	X	
8. Review and approve Wireless Access Services security architecture		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Design, test and implement approved Wireless Access Services architecture	X	
10. Deploy, manage, communicate and report on activities related to Wireless Access Services refresh	X	
11. Review and approve Wireless Access Services refresh report		X
12. Develop and implement Wireless Access Services policies and procedures	X	

*Schedule 4.3 – Operational Services*

---

<b>Wireless Access Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
13. Design, test and implement approved Wireless Access Services architecture	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
14. Provide support, including break-fix, for all Wireless Access Services assets	X	

## 5.11 Mobility VPN Access Services

### 5.11.1 Mobility VPN Access Services Overview

This section pertains to the Mobility VPN Access component provided within the Network Services Framework. Mobility VPN Access Resource Units will enable a persistent, secure, wireless connection to County networked applications by authorized County end-users who are working from remote locations. Contractor will provide the server hardware software and services, including licenses and 3<sup>rd</sup> party maintenance, needed to implement, train, maintain and support Mobility VPN Access services through the Mobility VPN Resource Unit. The Mobility VPN Access Resource Unit includes the components and resources needed to ensure the reliable functioning of the software that allows wireless access to County applications 7 days a week, 24 hours a day.

### 5.11.2 Mobility VPN Access Services - Feature/Benefit Descriptions

- 5.11.2.1 Maintain Connection-Mobility VPN Access will provide session persistence to end-users. This will eliminate repeat logins as workers cross network boundaries, go out of range, or suspend and then resume their devices. The service will handle wireless coverage gaps and roaming between networks.
- 5.11.2.2 End to End Security and Authentication-Mobility VPN Access will create a secure end-to-end tunnel that encrypts the complete data session from the Mobility server to the wireless device. All VPN users become authorized via enforced secure logins.
- 5.11.2.3 Disable Lost or Stolen Devices-Mobility VPN Access allows authorized Contractor administrators to disable the network access of lost or stolen wireless devices at the server or entry point into the County Network.
- 5.11.2.4 Training for County personnel will follow existing County procedures for activating existing Remote Access end-users. Contractor will provide website and e-mail instructions to end-users at time of software installation.
- 5.11.2.5 Break-Fix / IMAR.-Break/Fix call handling will comply with applicable MASLs. Single point of contact will be available for all installs, adds, moves and removes.

### 5.11.3 Mobility VPN Access Services Scope

Access will be provided to all employees authorized by the County for wireless (remote) application access.

**5.11.4 Mobility VPN Access Services Environment –**

**5.11.4.1 Hardware and Software**

All hardware, software and infrastructure will be provided by Contractor, to support Mobility VPN Access.

**5.11.4.2 Implementation**

The following is a list of tasks that will need to be performed to implement the Mobility VPN Access application on Desktop:

- Verification of Mobility VPN Access user PC requirements
- Provide web link to the CoSD intranet that will provide Net Motion client installation instructions
- Development and maintenance of help desk processes for Mobility VPN Access end-user support.

**5.11.5 Mobility VPN Access Services Requirements, Roles and Responsibilities**

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with Mobility VPN Access Services.

<b>Mobility VPN Access Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for a consolidated Mobility VPN Access services architecture	X	
2. Review and approve recommendations for Mobility VPN Access services architecture		X
3. Produce and submit Mobility VPN reporting requirements	X	
4. Review and approve Mobility VPN reporting requirements		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
5. Produce and submit operational policies and procedures for Mobility VPN Access services	X	
6. Review and approve operational policies and procedures for Mobility VPN Access services		X
7. Produce and submit plans for updates and patches for Mobility VPN Access assets	X	
8. Review and approve plans for updates and patches to Mobility VPN Access assets	X	
9. Design, test, and implement approved Mobility VPN Access services	X	

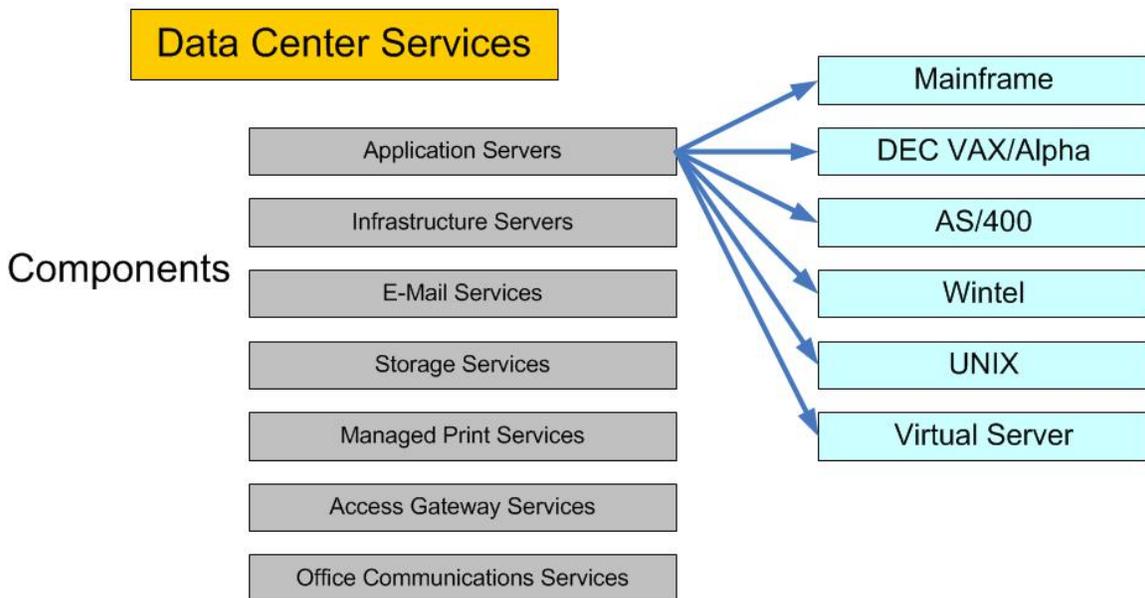
Mobility VPN Access Service: Plan, Build and Operate Requirements, Roles and Responsibilities		
10. Design and implement approved operational policies and procedures for Mobility VPN Access	X	
11. Design, test and implement approved plans for updates and patches to Mobility VPN Access services	X	
Operate Requirements, Roles and Responsibilities	Contractor	County
12. Provide support, including break-fix, for all Mobility VPN Access services	X	
13. Maintain, support and report on Mobility VPN Access services	X	
14. Review and approve report on Mobility VPN Access services		X
15. Maintain and support County of San Diego locations equipped with Mobility VPN Access services	X	
16. Maintain and support approved operational policies and procedures	X	

## 6 Data Center Services

### 6.1 Data Center Services Overview

This section pertains to the Data Center Services framework. Data Center Services consist of the Plan, Build and Operate services that include the assets, facilities and services associated with centralized, shared computing environment. Data Center Services are composed of the following components: Application Servers; Infrastructure Servers; E-Mail Service; Storage; ,Managed Print, Access Gateway Services and Office Communications Services.

### Service Framework



6.2 Data Center Services High Level Requirements

6.2.1 Data Center Services will be spread across multiple (two) Tier IV Contractor Data Centers with an appropriate split of application processing to achieve the following benefits:

6.2.2 Reduced business risk by having 50 percent of the priority applications in one facility

6.2.3 Reduced cost for disaster recovery services by using existing server capacity, rather than paying for idle servers, storage, and facilities

6.2.4 Simplified annual drills since processing is already available in each data center

6.2.5 Contractor will provide a single operations team across the dual data centers

6.2.6 Contractor will provide technology refresh, redundant systems and improved application architecture design

6.2.7 Contractor will provide technology assistance and support to the County in planning and standard-setting activities

6.2.8 Contractor will provide secure leveraged services where appropriate so the County will have the flexibility to quickly grow or reduce consumption, including:

6.2.9 Mainframe processing

6.2.10 Storage - Storage Area Network (SAN) and Network Attached Storage (NAS)

6.2.11 Centralized backups

6.2.12 Centralized monitoring

6.2.13 Maximize the efficient use of storage throughout the Data Center to minimize and eliminate underutilization of valued resources.

6.2.14 Maintain a stable, reliable infrastructure to support business applications throughout the County

6.2.15 Contractor shall publish all Data Center Services asset standards on the County Intranet

6.3 Data Center Services Environment

6.3.1 Contractor Facilities

**Schedule 4.3 – Operational Services**

Contractor will maintain and operate two (2) active Data Centers to support the County Data Center Services environment. Production application processing in the two Data Centers shall be split to enable timely recovery of Priority 1 and Priority 2 applications at one Data Center in the event of a disaster at the other Data Center.

**6.4 Data Center Services Requirements, Roles and Responsibilities**

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

<b>Data Center Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
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. Produce and submit recommended Data Center Services administration policies and procedures.	X	
8. Review and approve Data Center Services administration policies and procedures		X
9. Produce and submit operational documentation on system functions, change management, and Problem management processes.	X	
10. Review and approve operational documentation on system functions, change management, and Problem management processes.		X
11. Produce and submit recommendations on hardware standards for Data Center Services assets	X	
12. Review and approve hardware standards for Data Center Services assets		X
13. Produce and submit recommendation on software standards for Data Center Services assets	X	
14. Review and approve software standards for Data Center Services assets		X
15. Produce and submit recommendation for upgrades to Data Center Services assets as needed to meet business needs	X	
16. Review and approve upgrades to Data Center Services assets as needed to meet business needs		
17. Produce and submit plans for security updates to Data Center Services assets	X	
18. Review and approve plans for security updates to Data Center Services assets		X

*Schedule 4.3 – Operational Services*

<b>Data Center Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
19. Produce and submit yearly Data Center Services asset consolidation strategy	X	
20. Review and approve yearly Data Center Services asset consolidation strategy		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
21. Provide all design and engineering required to support Data Center Services Framework	X	
22. Produce and submit to County all design and engineering documentation	X	
23. Review and approval of all design and engineering documentation		X
24. Provide all test services required to support Data Center Services Framework	X	
25. Produce and submit to County all test documentation	X	
26. Review and approve all test documentation		X
27. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices)	X	
28. Deploy code and content using automated tools which include publishing, promoting, and rolling back code and content.	X	
29. Conduct deployment reviews and provide results to County	X	
30. Review and approve results of deployment reviews		X
31. Install security patches and security products	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
32. Provide support, including break-fix, for all Data Center Services assets	X	
33. Perform maintenance activities during non-peak hours (will be determined in coordination with the County)	X	
34. Provide the County with a system software upgrade list as it becomes available from software suppliers	X	
35. Measure, monitor, and adjust data center system and network parameters to make certain the required level of performance is maintained	X	
36. 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	

## 6.5 Application Server Services

### 6.5.1 Application Server Services Overview

This section pertains to the Application Server Services component within the Data Center Framework. The Application Server Services component applies to all hardware and software needed to maintain and support Application Servers. The physical Application Servers in the Data Center includes, but is not limited to, Mainframe, AS/400, VAX/VMS, Alpha, WINTEL, and UNIX servers. The software component defined will relate to the operating system standardization across the different Application Server types. Services provided within this component include, but are not

limited to, Application Server refresh, operating system update and support, management of server resources and server capacity analysis.

#### 6.5.2 Application Server Services High Level Requirements

6.5.2.1 Migrate or retire Applications on legacy, older obsolete Application Servers.

6.5.2.2 Contractor shall maintain currency of the operating systems on Application Server assets

6.5.2.3 Provide hardware refresh for specified Application Servers assets.

6.5.2.4 Provide hardware server consolidation recommendations, as well as, server migration recommendations to less expensive and more supportable hardware platforms.

6.5.2.5 Migrate Application Server storage to the centralized, shared storage environment (Section 6.8 of Schedule 4.3) for all refreshed Application Servers except Application Servers remaining on DASD (i.e. Mainframe, AS/400, VAX)

6.5.2.6 Maintain Application Test Servers to support the Application Development and integration process.

6.5.2.7 Provide centralized support for remote servers physically located offsite from the data center.

6.5.2.8 Perform backups to all Application Servers assets.

#### 6.5.3 Application Server Services Environment

The Application Server types include:

##### 6.5.3.1 Mainframe

Mainframe hardware standards are not applicable.

Mainframe will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated storage environment.

Contractor shall refresh the shared Mainframe on a 5 year refresh schedule, unless otherwise agreed to by the County in writing, based on a County-approved plan

that will minimize disruption and reduce risk. Refresh of the Mainframe may include periodic upgrades to key components that provide significant upgrades in functionality and performance, if approved by the County (e.g., CPU). Refresh of the Mainframe is not considered a billable Application Services task except for County-approved remediation of application software. If the operating system requires a hardware refresh the Contractor will perform this refresh as required with proper notification

#### 6.5.3.2 DEC VAX

DEC VAX hardware standards are not applicable. No additional DEC VAX hardware will be required to support the County. Current units will be phased out over a period of time to be determined by the County.

DEC VAX operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year. The process for determining updates to the operating system will be based on recommendations from the Contractor and approved by the County. The County intends to maintain currency with the operating system without major disruption or rework of the Application(s) hosted.

DEC VAX will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated storage environment.

There is no refresh for DEC VAX assets.

#### 6.5.3.3 VMS

VMS based Application Server (excludes DEC VAX) hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. Hardware standards will be set for three classes of server types: Small, Medium and Large. Some of the basic differences between small, medium and large servers will be number of CPUs, the speed or processing power of the CPUs, and the amount of memory installed. The process to set VMS based Application Server hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

VMS operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year.

Each Contract Year, 20% of the VMS based Application Servers will be refreshed. The refresh will occur over the course of the Contract Year using a straight line methodology (20% of assets evenly refreshed over 12 months). Hardware and operating system that meet current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process. Refresh of the VMS based Application Server is not considered a billable Application Services task except for County-approved remediation of application software

6.5.3.4 AS/400

AS/400 hardware standards are not applicable. No additional AS/400 hardware will be required to support the County. The current unit may be phased out over a period of time to be determined by the County.

AS/400 operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year.

AS/400 will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated storage environment.

There is no refresh for AS/400 assets.

6.5.3.5 Wintel

Wintel Application Servers hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The new hardware standards shall be stated in the Standards and Procedures Manual and shall be used for all new or refreshed servers during that Contract Year. Hardware standards will be set for three classes of server types: Small, Medium and Large. Some of the basic differences between small, medium and large servers will be number of CPUs, the speed or processing power of the CPUs, and the amount of memory installed. All Wintel Application Servers standards will be set with minimum storage installed. Application data storage will not be hosted on the Wintel Application Servers but will utilize the centralized, consolidated storage environment (Section 6.8 of Schedule 4.3). The process to set Wintel

Application Servers hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

Wintel Application Servers operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year. The process for determining updates to the operating system will be based on recommendations from the Contractor and approved by the County. The County intends to maintain currency with the operating system without major disruption or rework of the Application(s) hosted.

Each Contract Year, 20% of the Wintel Application Servers will be refreshed. The refresh will occur over the course of the Contract Year using a straight line methodology (20% of assets evenly refreshed over 12 months). Hardware that meets current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process. Refresh of the Wintel Application Server is not considered a billable Application Services task except for County-approved remediation of application software.

#### 6.5.3.6 UNIX

UNIX based Application Servers hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The new hardware standards shall be stated in the Standards and Procedures Manual and shall be used for all new or refreshed servers during that Contract Year. Hardware standards will be set for three classes of server types: Small, Medium and Large. Some of the basic differences between small, medium and large servers will be number of CPUs, the speed or processing power of the CPUs, and the amount of memory installed. All UNIX Application Servers standards will be set with minimum storage installed. Application data storage will not be hosted on the UNIX Application Servers but will utilize the centralized, consolidated storage environment (Section 6.8 of Schedule 4.3). The process to set UNIX based Application Servers hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

UNIX based Application Servers operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year. The process for determining updates to the operating system will be based on recommendations from the Contractor and approved by the County. The County intends to maintain currency with the operating system without major disruption or rework of the Application(s) hosted.

Each Contract Year, 20% of the UNIX based Application Servers will be refreshed. The refresh will occur over the course of the Contract Year using a straight line methodology (20% of assets evenly refreshed over 12 months). Hardware and operating system that meet current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process. Refresh of the UNIX Application Server is not considered a billable Application Services task except for County-approved remediation of application software.

#### 6.5.3.7 Virtual Server

6.5.3.7.1 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. The number of Virtual Guest servers per Virtual Host will be jointly determined by County and Contractor with the goal of obtaining maximum efficiencies without jeopardizing service delivery. Each Virtual Guest will be configured the same as standard physical servers and will receive the same type and level of monitoring and support as does a physical server. Virtual Guest Servers will be refreshed to maintain software currency based on current Contract year standards.

6.5.3.7.2 A Virtual Host Server is an X-Large Wintel Application Server. Hardware standards for Virtual Host Servers will be set annually with the process based on recommendations made by the Contractor and approved in writing by the County. The standard should be available from the manufacturer for the entire Contract Year. Refresh for the Virtual Host Servers will maintain an environment with assets not older than five (5) years from date of purchase.

#### 6.5.3.8 Class of Application Servers

##### 6.5.3.8.1 Application Production Servers

Application Production Servers host Portfolio Applications that are identified in the COSD Portfolio Catalog. Application servers also host such services as business rule execution, browser based presentation and database management systems. The Application Server becomes Production when the Portfolio Application is considered System of Record.

6.5.3.8.2 Application Pre-Production Servers

Application Pre-Production Servers are “in development” Application Servers that will be defined like Application Test Servers from the time of installation until completion of application development and integration as evidenced by customer acceptance of the new application.

6.5.3.8.3 Application Test Servers

Application Test Servers can be any defined class of Application Server specified within this section. The Test Server refers to a dedicated Application Server that is used in the test phase of the Application development and integration process. Application Test Servers will receive all the same services as any Application Server with the following exceptions: (1) return to service for break/fix for Application Test Servers will be within 48 hours, and (2) Backups will be performed weekly and backup tapes will be retained for one month.

6.5.3.9 Contractor Facilities

The Application Server Services will be performed across Contractor Data Centers.

6.5.3.10 Solaris Containers

Solaris Containers uses virtualization to allow for multiple -applications-per-physical server deployment model while sharing physical hardware resources. The objective is to safely consolidate multiple applications onto one physical system to increase utilization rates while decreasing costs associated with power, space, cooling, administrative and support costs.

A Solaris Container, much like any Virtual Guest Server, is a logical instance of the Solaris 5.10 or greater operating system and applications environment based on the use of virtualization software on a physical host server (x86 or SPARC). The number of Solaris Containers per physical Host will be jointly

determined by County and Contractor with the goal of obtaining maximum efficiencies without jeopardizing service delivery.

Each Solaris Container will be configured as if it were a physical server and will receive the same type and level of monitoring and support as does a physical server.

Solaris Containers will be refreshed to maintain software currency based on current Contract year standards.

Any use of Solaris Containers, whether Production or Preproduction/Test, will be approved by the County prior to installation.

**6.5.4 Application Server Services - Requirements, Roles and Responsibilities**

**6.5.4.1 Application Server Services Requirements**

Mainframe usage will be based on CPU hours. The Contractor must be able to correlate and report CPU hours directly to End-user processing.

**6.5.4.2 Application Server Services: Plan, Build and Operate Services Requirements, Roles and Responsibilities**

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

<b>Application Server Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for hardware standards of Application Server Services assets on a yearly basis	X	
2. Review and approve hardware standards for Application Server Services assets		X
3. Produce and submit recommendations for operating system standards for Application Server Services assets on a yearly basis	X	
4. Review and approve operating system standards for Application Server Services assets		X
5. Produce and submit Application Server Services refresh plan on a yearly basis	X	
6. Review and approve Application Server Services refresh plan		X
7. Produce and submit Application Server Services storage migration and consolidation plan on a yearly basis	X	
8. Review and approve Application Server Services storage migration and consolidation plan		X

**Schedule 4.3 – Operational Services**

<b>Application Server Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
9. Produce and submit backup/recovery polices and procedures	X	
10. Review and approve backup/recovery policies and procedures		X
11. Produce and submit recommendations for Application Server placement into County facilities	X	
12. Review and approve recommendations for Application Server placement into County facilities		X
13. Produce and submit recommendations for Application Server Services consolidation plan on a yearly basis.	X	
14. Review and approve Application Server Services consolidation plan.		X
15. Produce and submit Application Server Services assets plans for updates or patches as needed for reliable operations and to maintain security	X	
16. Review and approve Application Server assets Services plans for updates or patches as needed for reliable operations and to maintain security		X
17. Produce and submit recommendations for monitoring and exceptional conditions procedures.	X	
18. Review and approve monitoring and exceptional conditions procedures.		X
19. Produce and submit recommendations for job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs	X	
20. Review and approve job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs		X
21. Recommend replacement or upgrade of County utility software programs with commercially available software to support processing operations	X	
22. Produce and submit recommendations for standards on production jobs and Job Control Language (JCL)	X	
23. Review and approve recommendations for standards on production jobs and Job Control Language (JCL)		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
24. Provide all design and engineering required to deploy, refresh and support Application Server Services assets.	X	
25. Design, test and implement hardware standards for Application Server Services assets	X	
26. Design, test and deploy operating system standards for Application Server Services assets.	X	
27. Deploy, manage, communicate and report on activities related to Application Server Services refresh	X	
28. Review and approve reports on Application Server Services refresh		X
29. Design, test and execute Application Server Services storage migration and consolidation plan	X	
30. Implement approved backup/recovery policies and procedures	X	
31. Design, test and deploy approved Application Server Services consolidation plans	X	

**Schedule 4.3 – Operational Services**

<b>Application Server Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
32. Test and deploy approved updates or patches to Application Server Services assets	X	
33. Define test and demand batch scheduling requirements	X	
34. Prepare tests and Demand Batch Jobs for execution	X	
35. Execute test and Demand Batch Jobs on appropriate Servers	X	
36. Execute production batch jobs on appropriate Servers as defined by County schedules	X	
37. Implement scheduling tools for automating job execution	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
38. Provide support, including break-fix, for all Application Server Services assets	X	
39. Manage and maintain Application Server Services test environment	X	
40. Provide support for Application Servers located in County Locations	X	
41. Provide support for Application Pre-Production and Application Test Servers	X	
42. Provide support for Application Server Services storage migration and consolidation plan	X	
43. Perform backups on Application Servers assets as defined	X	
44. Conduct data and Application migration that is necessary due to any Application Server refresh or break-fix activity	X	
45. Manage the migration of production jobs to the JCL and program libraries	X	
46. Provide job scheduling, job execution, reporting and resolution	X	
47. Manage scheduling tools for automating job execution (e.g., job workflow processes, interdependencies, County contacts, and rerun requirements file exchange functions and print management)	X	
48. Monitor progress of scheduled jobs and identify and Resolve issues in scheduling process	X	
49. Schedule and process special job requests	X	
50. Restart failed jobs to ensure completeness.	X	
51. Maintain documentation of job scheduling, contact, rerun and interdependencies/dependency structures.	X	
52. Maintain, and utilize, an emergency contact list and escalation procedures to Resolve Abnormal Endings (ABENDs)	X	
53. Resolve abnormal terminations caused by conditions external to production programs	X	
54. Review on a daily basis all batch/schedule Failures to determine root cause and ensure a permanent solution is applied	X	
55. Notify County and maintain a history of job completion results	X	
56. Assess the processing time for each batch application and identify where run-time improvements can be made in areas such as shortening a job flow's critical path, reducing the run-time for specific jobs, and reducing the overall number of jobs to process on an initial and ongoing basis	X	

**Schedule 4.3 – Operational Services**

---

<b>Application Server Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
57. Provide input processing, for activities such as loading third-party tape and receipt and/or transmission of batch files	X	
58. Support send and receive electronic data transmissions (e.g., EDI, FTP)	X	
59. Perform upgrades to Application Server Services assets	X	
60. Monitor, operate, maintain and support OS (Operating Systems) installed on Application servers	X	
61. Monitor, operate, maintain and support the 3 <sup>rd</sup> party Applications running on Application servers	X	
62. .Execute standard operating procedures at scheduled times	X	
63. Start-up and shut-down County online/interactive systems according to defined schedules or upon approved requests	X	
64. Coordinate and manage 3 <sup>rd</sup> -party vendor hardware and software maintenance to meet County requirements	X	
65. Ensure that System management and monitoring tools do not impact County operations	X	
66. Provide automated event monitoring tools that will notify Applications Team for immediate response if there is an application-related problem	X	

6.6 Infrastructure Services

6.6.1 Infrastructure Services Overview

This section pertains to the Infrastructure Services component within the Data Center Framework. The Infrastructure Services component applies to all hardware and software needed to maintain and support a distributed network environment. Services provided within this component include, but are not limited to, server deployment and maintenance, server refresh, server tuning and monitoring, software distribution, and systems management. Additional network services within this component include, but are not limited to, DNS, DHCP, End-user Authentication, directory services, software distribution, system management, print servers, ftp, certificate servers, proxy services, web filtering and any Contractor internal servers/services needed to support the environment. Servers that support the Infrastructure Service component can be UNIX or Windows based and will be dependent on the service being provided.

6.6.2 Infrastructure Services High Level Requirements

6.6.2.1 Contractor shall provide update and support for a distributed network environment

6.6.2.2 Contractor shall provide centralized and standardized system that automates network management of user data, security, and distributed resources

6.6.2.3 Contractor shall automate software distribution including delivering applications, images, and patches to the environment using industry standard tools.

6.6.2.4 Contractor shall provide an easy to use, secure and responsive End-user authentication methodology

6.6.2.5 The Infrastructure Services, hardware and software, must be designed and maintained to support business strategy and applications

6.6.2.6 Contractor shall support and maintain the Public Library public infrastructure

### 6.6.3 Infrastructure Services Environment

#### 6.6.3.1 Hardware and Software

Infrastructure Server (UNIX or Intel) hardware standards will be determined yearly and updates to hardware will go into effect at the start of each Contract Year. The new hardware standards shall be stated in the Standards and Procedures Manual and shall be used for all new or refreshed servers during that Contract Year. Hardware standards will be set for three classes of server types: Small, Medium and Large. Some of the basic differences between small, medium and large servers will be number of CPUs, the speed or processing power of the CPUs, and the amount of memory installed. The process to set Infrastructure Server hardware standards will be based on recommendations made by the Contractor and approved in writing by the County. Each model selected for a standard should be available from the manufacturer for the entire Contract Year.

Infrastructure Server operating system revisions will be reviewed annually prior to the subsequent Contract Year (at least 60 days prior to start of new Contract Year) and updates will go into effect at the start of each Contract Year. The process for determining updates to the operating system will be based on recommendations from the Contractor and approved by the County. The Contractor will maintain software (including operating system) on Infrastructure servers within one (1) year but not earlier than three (3) months after the release date of the software.

Infrastructure Servers will be configured with their own specific storage and will not be integrated into the centralized, consolidated storage environment (Section 6.8 of Schedule 4.3). The infrastructure servers will not be considered End-user file storage systems.

Each Contract Year, 20% of the Infrastructure Servers will be refreshed, unless otherwise approved in writing by the County, and will include the Public Library public infrastructure. The refresh will occur over the course of the Contract Year using a straight line methodology (20% of assets evenly refreshed over 12 months). Hardware that meets current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process

#### 6.6.3.2 Contractor Facilities

**Schedule 4.3 – Operational Services**

The Infrastructure Services will be performed across both active Contractor Data Centers. Additional Infrastructure Servers may be placed in County sites as needed to meet the MASLs

**6.6.4 Infrastructure Services Requirements, Roles and Responsibilities**

**6.6.4.1 Infrastructure Services Requirements**

Infrastructure Servers used for the delivery of Services in E-Mail Services (Section 6.7 of Schedule 4.3) and Storage Services (Section 6.8 of Schedule 4.3) are not included within this section. These servers are specified and supported within their respective section.

**6.6.4.2 Infrastructure Services: Plan, Build and Operate Requirements, Roles and Responsibilities**

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

<b>Infrastructure Servers Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
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 County facilities	X	
4. Review and approve recommendations for Infrastructure Server placement into County facilities		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
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

**Schedule 4.3 – Operational Services**

<b>Infrastructure Servers Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
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
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
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	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
23. Provide support, including break-fix, for all Infrastructure Server Services assets	X	
24. Provide support for Infrastructure Servers located in County facilities	X	
25. Conduct data and Infrastructure migration that is necessary due to any Infrastructure Server Services refresh or break-fix activity	X	
26. Perform upgrades to Infrastructure Server Services assets	X	
27. Monitor, operate, maintain and support OS (Operating Systems) installed on Infrastructure Server Services assets.	X	
28. Manage Infrastructure Server Services to meet performance Minimum Service Levels	X	
29. Maintain and support the Public Library public infrastructure web filtering	X	
30. Manage bandwidth and latency constraints and minimize impacts during automated software deployment	X	
31. Provide deployment services using automated tools for remote access/VPN users	X	
32. Provide deployment reports to include success and failure statistics of scheduled distributions — such as patches or upgrades	X	

## 6.7 E-Mail Services

### 6.7.1 E-Mail Services Overview

This section pertains to the Electronic Mail (E-mail) Services component within the Data Center Framework. The E-Mail Services component applies to all hardware and software needed to maintain and support Electronic Mail. The E-Mail system will be based on Microsoft Exchange. Services provided within this component include, but are not limited to, E-Mail account management, refresh, Exchange software updating and support, management of E-Mail server resources, server capacity analysis and server and storage consolidation. E-Mail services includes all the components needed to ensure reliable and uninterrupted delivery of E-Mail to County End-Users, these services include, but are not limited to, E-Mail relays, Blackberry Enterprise Services, Web Access Servers, Proxy Servers, E-Mail servers, Fax Servers, user based e-mail encryption services and all supporting E-Mail services assets.

### 6.7.2 E-Mail Services High Level Requirements

6.7.2.1 Provide a split Active Directory/Exchange server environment between the two data centers to allow for a disaster recovery of the Exchange environment from either facility.

6.7.2.2 Provide perimeter services that will protect against SPAM and E-Mail Worms or malicious software

6.7.2.3 Support secure remote access to E-Mail resources to authorized users.

6.7.2.4 Refresh and update E-Mail resources to meet service levels and capacity

6.7.2.5 Maintain the E-Mail environment within one version of the latest release of Microsoft Exchange.

6.7.2.6 Synchronize E-Mail directories with all County Departments (e.g. Sheriff, District Attorney, DCSS) Integrate fax capability into E-Mail desktop client for receipt and transmission

6.7.2.7 E-mail encryption may be ordered on a per user basis to provide encryption of E-mails sent outside the County network. Contractor shall:

6.7.2.7.1 Provide ability to send encrypted emails to email addresses outside of the County network.

6.7.2.7.2 Provide external recipients of encrypted e-mails with the ability to access encrypted e-mail content via a authentication.

6.7.2.7.3 Provide a help desk service to receive assistance with the encrypted e-mail.

6.7.2.7.4 Provide County senders of encrypted e-mail with the ability to request and receive system-generated Read Receipts.

6.7.2.7.5 Provide the ability for County senders of encrypted e-mail to lock or otherwise prevent a message from being read by a recipient after the message has been sent.

6.7.2.7.6 Permit County users to establish an Expiration date after which messages they have sent cannot be opened.

6.7.2.7.7 Provide self-help password administration for recipients of encrypted emails that will permit passwords to be established and reset by end user recipients.

6.7.2.7.8 Provide a profile-driven implementation of encryption functionality. Deploy two initial profiles, one to encrypt all outgoing mail unless the County user de-selects encryption and a second profile to not encrypt any outgoing email unless the user selects the encryption option.

### 6.7.3 E-Mail Services Environment

#### 6.7.3.1 Hardware and Software

E-Mail Servers (UNIX or Intel) hardware standards will be based upon standards established for Infrastructure Services in section

E-Mail Servers operating system revisions will be based upon standards established for Infrastructure Services in section 6.6.3.1. The E-Mail application, Microsoft Exchange, will be maintained to within one version of the current released product. The Exchange servers will be patched and updated as needed to ensure continuous reliable transport of E-Mail to and from County End-Users.

The County's current e-mail environment will be consolidated at time of transition into Exchange 2003, split between the two primary data centers to allow for a built in disaster recovery function. The Services will include the spam and

virus filtering provided by an appliance device. The End User mailbox shall be in accordance with the County’s e-mail retention policy.

Each Contract Year, 20% of the E-Mail Servers will be refreshed, unless otherwise agreed by the County in writing. The refresh will occur over the course of the Contract Year using a straight line methodology (20% of assets evenly refreshed over 12 months). Hardware and operating system that meet current Contract Year standards (defined on an annual basis during the preceding Contract Year) will be deployed as part of the refresh process.

**6.7.3.2 E-Mail Services Requirements, Roles and Responsibilities**

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with E-Mail Services.

<b>E-Mail Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit Email Services operational and computing procedures.	X	
2. Review and approve Email Services operational and computing procedures.		X
3. Produce and submit Email Services architecture	X	
4. Review and approve Email Services architecture		X
5. Produce and submit recommendations for Exchange application standards on a yearly basis.	X	
6. Review and approve Exchange application standards		X
7. Produce and submit Email Server refresh plan on a yearly basis	X	
8. Review and approve Email Server refresh plan.		X
9. Produce and submit recommendations for consolidating Exchange servers	X	
10. Review and approve recommendations for consolidating Exchange servers		X
11. Produce and submit backup/recovery policies and procedures	X	
12. Review and approve backup/recovery policies and procedures		X
13. Produce and submit defining policies and procedures for functions including email, calendaring and mail messaging delivery components	X	
14. Review and approve policies and procedures for functions including email, calendaring and mail messaging delivery components		X
15. Produce and submit plans to update and patch Email Services to maintain reliability and security	X	
16. Review and approve plans to update and patch Email Services to maintain reliability and security		X

**Schedule 4.3 – Operational Services**

<b>E-Mail Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
17. Produce and submit procedures for directory synchronization with County departments	X	
18. Review and approve procedures for directory synchronization with County departments		X
19. Produce and submit plans and procedures to protect County End-users from SPAM, Email Worms or malicious software.	X	
20. Review and approve plans and procedures to protect County End-users from SPAM, Email Worms or malicious software.		X
21. Produce and submit End-user tip sheets on use of Email services.	X	
22. Develop procedures for email encryption to be added to change in or deleted from a user’s account after the initial implementation of the encryption function.	X	
23. Review and approve plans and procedures to allow County End-Users to encrypt Emails to external addresses.		X
24. Produce and submit End-user tip sheets on use of Email services including encryption.	X	
25. Review and approve for distribution End-user tip sheets on use of Email services		X
26. Produce and submit plans for Email integrated Fax solution	X	
27. Review and approve Email integrated Fax solution		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
28. Design and implement Email Services operational and computing procedures	X	
29. Design, test and implement approved changes to the Exchange application.	X	
30. Design, test and deploy Email server refresh according to the approved plan.	X	
31. Design, test and implement approved plans for consolidation of Exchange servers or Exchange storage	X	
32. Design and implement policies and procedures for functions including email, calendaring and mail messaging delivery components	X	
33. Design, test and implement approved updates and patches to E-Mail Services.	X	
34. Design, test and implement directory synchronization with out-of-scope County departments.	X	
35. Design, test and implement approved plans and procedures to protect County End-users from SPAM, Email Worms or malicious software.	X	
36. Design, test and implement approved plans and procedures to be used by Data Center in order to allow County End-Users to encrypt email being sent to external addresses.	X	
37. Provide encryption plug-ins for Outlook clients	X	
38. Deploy and install encryption profiles to email encryption end users	X	

**Schedule 4.3 – Operational Services**

<b>E-Mail Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
39. Implement approved backup/recovery policies and procedures	X	
40. Distribute End-user approved tip sheets	X	
41. Implement Email retention policies	X	
42. Design and implement E-mail integrated Fax solution	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
43. Provide support, including break-fix, for all Email Services assets	X	
44. Manage and support Email Services to meet operational and computing procedures.	X	
45. Manage and support Exchange application	X	
46. Support and provide Email accounts to End-users	X	
47. Provide and support migration of End-user mailboxes in support of Email server refresh or break-fix activity	X	
48. Manage and support directory synchronization operations	X	
49. Manage and support SPAM services and other specific services needed to protect End-users	X	
50. Manage and maintain Email accounts, Blackberry accounts, and Email SMTP addresses	X	
51. Manage and support Email encryption services	X	
52. Manage and maintain Email Services to Minimum Service Levels	X	
53. Perform backups on Email Services Servers assets as defined	X	
54. Support e-mail retention policies	X	
55. Manage and support integrated Fax Services	X	
56. Produce encryption RU reports monthly	X	
57. Manage and Maintain email encryption accounts for end users	X	

**6.8 Storage Services**

**6.8.1 Storage Services Overview**

This section pertains to the Storage Services component within the Data Center Services Framework. There are three primary categories of data storage:

6.8.1.1 Attached Storage –Applies to all storage used to store End-user Data that is directly attached to a physical Application Server and includes Mainframe, VAX, VMS, AS/400, UNIX and WINTEL Application Servers.

6.8.1.2 Shared Storage Services - this applies to a centralized and consolidated storage environment for End-user Data and includes Storage Area Network (SAN), and Network Attached Storage (NAS).

6.8.1.3 Immutable Storage – this applies to a dedicated storage environment for maintaining a legal copy of records that are not modifiable or changeable, they are immutable (for example the County’s Assessor Recorder County Clerk (ARCC) Recording System). This environment will be replicated between the two data centers to further meet legal requirements. Immutable storage consists of two (2) storage systems, one deployed in the Plano data center and one deployed in the Tulsa data center. The current configuration shall support Bi-direction replication. Bi-directional replication allows user to write to either of the two storage systems and have data copied to the other. Therefore, data written on storage system A in Tulsa shall be replicated to storage system B in Plano, and vice versa. .

Immutable Storage will be dedicated to the County of San Diego, and not leveraged with any other non-County client

Services provided within the Storage Services component include, but are not limited to, end-user access, recovery (via backup and replication) of all Storage Services assets, data protection, storage reporting to the business unit, low org or end-user, storage capacity analysis, and storage management. In addition, services provided within the Storage Services include, but are not limited to, storage consolidation, tiered storage and migration from Attached Storage to centralized Storage Services where appropriate.

Attached Storage is the directly attached storage that resides on legacy Application Servers. The purpose of this storage type is for those Application Servers that exist in the environment, will not be immediately refreshed and contain End-user data. As Application Servers are refreshed End-user data will be migrated from Attached Storage to Shared Storage unless there are specific technical reasons why the End-user data must remain on Attached Storage.

The Shared Storage Services infrastructure shall be a centralized, integrated, tiered repository for County generated data. The purpose of the Shared Storage Services infrastructure is the elimination of storage underutilization, avoidance of “islands of storage”, a decrease in overall recovery time and efficiency of storage administration and management (including management of storage capacity). Application Servers, as they are refreshed or newly acquired, shall be integrated into the Shared Storage Services infrastructure.

Shared Storage Services will be broken down into levels or types of storage.

- Level 1 will be high-performing storage technology with a high degree of I/O performance, and will contain mission critical data for business operations.
- Level 2 will be low cost, high capacity storage that does not require a high degree of I/O performance and/or is viewed as non-mission critical to business operations and may be considered near-line storage.
- Level 3 Storage – Shared Immutable Storage is replicated storage for the lifecycle management of records that are not to be modified.
- Tier III is archive storage managed through a File Management Appliance (FMA). The FMA provides automated policy management to move files to lower cost storage destinations.

The current configurations for each of the Level 1 and Level 2 and Tier III storage services utilize a shared SAN and backup environment.

The specific service definitions are listed below. Changes to these configurations will be mutually agreed upon over the term of the Agreement as technology changes.

- Level 1 Storage – Shared Storage Environment using– Raid 5 High Performance Drives
- Level 2 Storage – Shared Storage Environment using– Raid 5 Lower Performance Drives
- Level 3 Storage – Shared Immutable Storage using the replicated immutable storage devices as approved by the County.
- Tier III Storage – Shared Storage Environment using low cost network storage devices .as approved by the County.

Storage Services will be measured by installed, usable capacity which does not include any data replication or other storage requirements necessitated by the Contractor's Disaster Recovery or backup and recovery solutions. The replication of immutable storage is not considered part of this exclusion since it is a required feature of this type of storage. The growth of storage capacity throughout the County needs to be predictable and managed. Unmanaged data growth should be eliminated throughout the storage infrastructure by implementing storage management and

storage reporting. Additional capacity to the shared storage environment, by level, will be proposed by the Contractor and approved by the County.

6.8.2 Storage Services High Level Requirements

6.8.2.1 Develop a consolidated and centralized storage environment

6.8.2.2 Provide dedicated Content Addressed Storage (CAS) specifically for immutable data for the County of San Diego.

6.8.2.3 Implement storage management processes and procedures

6.8.2.4 Produce Storage Service reports by Storage type and level down to the business unit, department and End-user.

6.8.2.5 Enable efficient and effective Storage Services management reporting to the business unit, department and End-user

6.8.2.6 Implement centralized control and management of the Storage Services infrastructure

6.8.2.7 Lower hardware and software maintenance costs associated with Shared Storage Services

6.8.2.8 Manage data backups of Storage Services assets with the intent to decrease recovery time

6.8.2.9 Provide automated backups over a network connection to the backup site where required to meet recovery times

6.8.2.10 Provide secure and bonded transportation and offsite storage of backups

6.8.2.11 Attached Storage Services assets shall be refreshed on the same cycle as its associated Application Server unless migrated to Shared Storage

6.8.2.12 Shared Storage Services shall be refreshed at least every five (5) years based on Contractor's refresh schedule of the shared storage environment and upon prior notification to and approval of the County

### 6.8.3 Storage Services Environment

The Storage Services environment will include data from:

#### 6.8.3.1 End-User Data

End-user Data would be the data generated by a County Portfolio Application used to deliver business value to the County or its customers and stored typically on Application Servers. Other End-user data are files generated by County End-users on Desktop Services assets using typically Office Automation tools such as Word, Excel and PowerPoint. This data is broken down into various types, such as, user home drives, department share drives, and enterprise share drives

#### 6.8.3.2 Mainframe

Mainframe will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated shared storage environment

#### 6.8.3.3 DEC VAX

DEC VAX will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated shared storage environment

#### 6.8.3.4 VMS

Refreshed or newly acquired VMS based servers will be migrated into the Shared Storage Services. VMS based servers are refreshed at a rate of 20% a year, so the expectation is that Storage consolidation will be achieved within five (5) years.

#### 6.8.3.5 AS/400

AS/400 will continue to utilize DASD for storage requirements and will not be part of the centralized, consolidated shared storage environment

#### 6.8.3.6 Wintel

Refreshed or newly acquired Wintel Application Servers will be migrated into the Shared Storage Services. Wintel Application Servers are refreshed at a rate of 20% a year, so the expectation is that Storage consolidation will be achieved in no more than five (5) years

#### 6.8.3.7 UNIX

**Schedule 4.3 – Operational Services**

Refreshed or newly acquired UNIX Application Servers will be migrated into the Shared Storage Services. UNIX Application Servers are refreshed at a rate of 20% a year, so the expectation is that Storage consolidation will be achieved in no more than five (5) years

**6.8.3.8 CAS**

Dedicated CAS environment will be utilized for County immutable storage requirements

**6.8.4 Storage Services Requirements, Roles and Responsibilities**

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

<b>Storage Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations on Shared Storage Services Architecture	X	
2. Review and approve recommendations on Shared 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 Services consolidation and Application Server migration to Shared Storage Service environment on a yearly basis.		X
5. Produce and submit Storage Services management policies/procedures.	X	
6. Review and approve Storage Services management policies/procedures.		X
7. Produce and submit Storage Services reporting policies/procedures.	X	
8. Review and approve Storage Services reporting policies/procedures.		X
9. Produce and submit Storage Services policies and procedures	X	
10. Review and approve Storage Services policies and procedures		X
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 County Storage demands.	X	
14. Review and approve plans for meeting County 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

**Schedule 4.3 – Operational Services**

<b>Storage Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
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 Shared Storage	X	
21. Review and approve plans to add additional Shared Storage		X
22. Produce and submit a data management strategy that will make certain that commonly used data has a defined minimum set of characteristics that include the following: <ul style="list-style-type: none"> <li>• Definition of the data object (what is it?)</li> <li>• Reference (where and how is the data object used?)</li> <li>• Metadata (data object attributes, such as type, size, and range of values)</li> <li>• Ownership and governance (who owns data, definitions, content, and so on?)</li> </ul>	X	
23. Review and approve data management strategy		X
24. Implement that strategy using an Information Lifecycle Management (ILM) approach to storing the data. Service shall be delivered for the most prominent applications that benefit from early adoption of ILM.	X	
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. This rationalization will reduce the County’s data storage costs through the following: <ul style="list-style-type: none"> <li>• Leveraging centralized hardware</li> <li>• Reducing administrative costs by reducing the number of databases</li> <li>• Providing centralized data repository</li> <li>• Reducing costs by reducing under-utilized storage</li> <li>• Reducing and eliminating autonomous backup and recovery solutions for centrally administered and managed backup and recovery</li> </ul>	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
26. Design and Implement recovery processes based on approved policies/procedures	X	
27. Design and Implement Storage management processes based on approved policies/procedures	X	
28. Implement Storage Services Reporting	X	
29. Design and Implement Storage consolidation based on approved recommendations.	X	
30. Deploy, manage, communicate and report on activities related to Storage Services refresh	X	
31. Review and approve Storage refresh report		X
32. Design and Implement Storage provisioning and allocation processes based on approved policies	X	
33. Design and implement capacity management	X	

**Schedule 4.3 – Operational Services**

<b>Storage Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
34. Implement approved Storage Services policies and procedures	X	
35. 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	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
36. Provide support, including break-fix, for all Storage Services assets	X	
37. Manage and support the Storage Services	X	
38. Produce and submit monthly Storage Services reports	X	
39. Review and approve monthly Storage Services reports		X
40. Support Storage Services refresh	X	
41. Perform and support media management activities for Storage Services	X	
42. Manage and support the media requests	X	
43. Perform tapes mounts as required	X	
44. Perform special tape shipments as requested	X	
45. Load and manage third-party media as required	X	
46. Prepare and manage media for use by microfiche service	X	
47. Manage and perform file transfers and other data movement activities related to break/fix or consolidation of Storage assets	X	
48. Perform data backups of Storage Services per approved policies and procedures	X	
49. Perform recovery processes on Storage assets	X	
50. Perform storage utilization management	X	
51. Manage and maintain all Storage assets and services	X	
52. Manage and maintain backup media library	X	
53. Manage and maintain the Storage Services Assets	X	
54. Produce and submit Storage Management Reports	X	
55. Review and accept Storage Management Reports.		X

**6.9 Managed Print Services**

**6.9.1 Managed Print Services Overview**

This is the section pertains to the Managed Print Services component within the Data Center Framework. The Managed Print Services 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

**Schedule 4.3 – Operational Services**

6.9.2 Managed Print Services High Level Requirements

6.9.2.1 Maintain reliable Managed Print Operations that allows County business to continue uninterrupted

6.9.2.2 Lower overall Managed Print cost by increasing overall efficiencies

6.9.3 Managed Print Services Requirements, Roles and Responsibilities

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

<b>Managed Print Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit output management requirements, policies, and procedures including transport, delivery locations and schedule requirements	X	
2. Review and approve output management requirements, policies, and procedures		X
3. Produce and submit automated output distribution requirements	X	
4. Review and approve automated output distribution requirements		X
5. Produce and submit recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.	X	
6. Review and approve recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
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	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
10. Provide support, including break-fix, for all Managed Print assets		
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 Minimum Service Levels	X	

<b>Managed Print Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
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	

## 6.10 Access Gateway Services

### 6.10.1 Access Gateway Services Overview

This section pertains to the Access Gateway Services component within the Data Center Framework. The Access Gateway Services component is a secure application access solution providing users with remote access from anywhere into County Data Centers. The Access Gateway Services component encompasses all hardware, software and services needed to implement, maintain and support the Access Gateway.

### 6.10.2 Access Gateway Services High Level Requirements

6.10.2.1 The Access Gateway Services will provide application-level access control for users from any location outside the County IT perimeter

6.10.2.2 The Access Gateway Services will provide a single point of secure remote access with a single set of logon credentials.

6.10.2.3 The Access Gateway Services will provide support for initially 1,400 remote users, with a maximum number of 4,300 remote users planned

6.10.2.4 The Access Gateway Services will be used to support the Anasazi application only.

6.10.2.5 Contractor shall refresh Access Gateway Services assets on a 5 year refresh schedule, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that will minimize disruption and reduce risk.

### 6.10.3 Access Gateway Services Requirements, Roles and Responsibilities

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

<b>Access Gateway Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for a Data Center based application centric Access Gateway Services architecture	X	

**Schedule 4.3 – Operational Services**

<b>Access Gateway Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
2. Review and approve recommendations for Access Gateway Services architecture		X
3. Produce and submit operational policies and procedures for Access Gateway Services	X	
4. Review and approve operational policies and procedures for Access Gateway Services		X
5. Produce and submit plans for updates and patches to Access Gateway assets	X	
6. Review and approve plans for updates and patches to Access Gateway assets		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Design, test and implement approved Access Gateway Services	X	
8. Design and implement approved operational policies and procedures for Access Gateway Services	X	
9. Design, test and implement approved plans for updates and patches to Access Gateway assets	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
10. Provide support, including break-fix, for all Access Gateway Services assets	X	
11. Maintain, support and report on Access Gateway Services	X	
12. Review and approve reporting on Access Gateway Services		X
13. Maintain and support approved operational policies and procedures	X	
14. Implement and Install all approved updates and patches	X	

**6.11 Office Communications Services**

**6.11.1 Office Communications Services Overview**

This section pertains to the Office Communications Service (OCS) provided within the Data Center Framework. The Office Communications Service component applies to all hardware and software needed to maintain and support Office Communications, whether housed in the Data Center or distributed to Desktop Assets. The Office Communications Services will be based on Microsoft Office Communication Server (OCS) software. Services provided within this component include Office Communicator account management, refresh, OCS software updating and support, management of Office Communication server resources, server capacity analysis and server and storage consolidation. The Office Communications Service offering includes all the components needed to ensure reliable and uninterrupted delivery of Office Communications to County End-users. These services are exclusively Dedicated Real-Time Collaboration Services, Synchronous Text Exchange, Presence Awareness, Peer-to-Peer Collaboration, Audio/Video Capability, Communicator Web Access, Web Conferencing (Live Meeting), RIM Mobile Access, and Utilization Reporting.

All services are provided only to accounts within the sdcounty.ca.gov domain (internal access only)

#### 6.11.2 Office Communications Services High Level Requirements

##### 6.11.2.1 Initial Build

Provide an initial build of the Office Communication Services (OCS) infrastructure.

##### 6.11.2.2 Dedicated Real-Time Collaboration Services

Provide the infrastructure to enable client applications to publish and subscribe to extended or enhanced presence information. Invite additional live parties to a two-person IM conversation, send an instant message to multiple parties and send an instant message to a Microsoft Exchange Server distribution list.

##### 6.11.2.3 Synchronous Text Exchange

Provide the ability for users to exchange text messages in real time (chat). The logging of text exchanges will be administratively disabled by the system.

##### 6.11.2.4 Presence Awareness

Provide the ability for a user to immediately detect another user's availability.

##### 6.11.2.5 Peer to Peer Collaboration

Provide the ability for users to share text, files, whiteboards and presentations.

##### 6.11.2.6 Audio/Video Capability

Microsoft Office Communications Service software provides users the ability to specify the addition of audio/visual capability when scheduling a conference as well as the ability to add audio or video to an existing IM conversation or conference call. Multiparty audio and video sessions will be handled by the OCS A/V Conferencing Server.

A/V capability under this OCS resource unit will be limited to users at County sites serviced by OptiMan and GigaMan circuits. This limitation will be established and administered via Group Policy in Active Directory at the Individual, Group or Site level as mutually agreed to by the County and Contractor. If further limitations on A/V become necessary, Contractor will establish a reverse QOS statement on the LAN link at a level mutually agreed to by the County and the Contractor. Both Audio and Video functionality will be non-enterprise, non-business quality with no

performance commitments associated with these capabilities. Audio capability provided via OCS will not support offnet calling or voicemail integration.

Recording of both of audio and video will be administratively disabled by default by the system. Due to the complexity of the drivers required, A/V installation and setup will be supported only on peripherals tested by Desktop Engineering as part of the Catalog approval process.

#### 6.11.2.7 Communicator Web Access

Provide Communicator functionality (Instant Messaging services through a browser client) via a web presence inside the COSD network. Allow users the ability to do Instant Messaging (text only) using Internet Explorer (IE) without requiring the installation of a client.

#### 6.11.2.8 Web Conferencing (Live Meeting)

Provide the ability for conference data collaboration including native support for Microsoft Office PowerPoint presentations, Microsoft Office document sharing, white boarding, application sharing, polling, Q&A, compliance logging, annotations, meeting summaries, handouts and various multimedia formats. Recording of the both of audio and video components of Live Meetings will be administratively disabled by the system.

#### 6.11.2.9 RIM Mobile Access

Provide the ability for clients to do IM and Presence using BlackBerry devices. This plug in module will be implemented to include integration of the BES (Blackberry Backend Server) to the OCS server

#### 6.11.2.10 Utilization Reporting

OCS end user utilization reports will be made available to the County monthly using the standard reporting capabilities that exist with the OCS software.

**6.11.3 Office Communications Services Environment**

The OCS Servers will be based upon standards and server refresh requirements as defined in Section 6.6 Infrastructure Services of Schedule 4.3.

OCS non-operating system software (initially Microsoft Office Communication Server) will be provided by the County and will be maintained at a minimum level of n-1 to the current released version. Changes to the Office Communications Services environment will be based on recommendations from the Contractor and approved by the County.

OCS Servers will be configured with their own specific storage and will not be integrated into the centralized, consolidated storage environment. The OCS servers will not be considered End-user file storage systems. If recording of either the Audio/Video capability or the Web Conferencing capability as described Schedule 4.3 is enabled by the County, these recordings will not be stored on the OCS Servers. If these sessions are stored on the network, they will be treated as either Level 1 or Level 2 storage and will be considered billable attached storage.

**6.11.4 Office Communications Services Requirements, Roles and Responsibilities**

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

<b>Office Communications Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit OCS operational and computing procedures	X	
2. Review and approve OCS operational and computing procedures		X
3. Produce and submit OCS architecture	X	
4. Review and approve OCS architecture		X
5. Produce and submit recommendations for OCS standards on a yearly basis.	X	
6. Review and approve OCS 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 OCS functions	X	
10. Review and approve policies and procedures for OCS functions		X
11. Produce and submit plans to update and patch OCS architecture to maintain reliability and security	X	

**Schedule 4.3 – Operational Services**

<b>Office Communications Service: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
12. Review and approve plans to update and patch OCS architecture to maintain reliability and security		X
13. Produce End-user tip sheets on use of OCS services. Provide tip sheets to CTO for distribution to County end users.	X	
14. Review and approve for distribution End-user tip sheets on use of OCS services		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
15. Design and implement OCS operational and computing procedures	X	
16. Design, test and implement approved changes to the OCS architecture	X	
17. Design, test and implement approved plans for consolidation of OCS (OCS) servers or storage	X	
18. Write and implement Help Desk scripts for Desktop support of OCS services.	X	
19. Design, test and deploy OCS server refresh according to the approved plan.	X	
20. Design and implement policies and procedures for functions including IM, Live Messaging and A/V conferences.	X	
21. Design, test and implement approved updates and patches to OCS Services	X	
22. Implement approved backup/recovery policies and procedures	X	
23. Review and approve OCS operation and computing procedures, refresh, changes to OCS architecture, plans for consolidation of OCS servers and storage.		X
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
24. Provide support, including break-fix, for all OCS assets	X	
25. Manage and support OCS to meet operational and computing procedures	X	
26. Manage and support the Microsoft Office Communications application	X	
27. Support and provide OCS functionality to End-users as authorized and requested	X	
28. Perform backups on OCS Servers assets	X	
29. Provide monthly utilization reports using the standard reporting capabilities that exist with the OCS software	X	
30. Manage and support OCS integration with Active Directory	X	

## **7 Cross Functional Services**

### **7.1 Cross Functional Services Overview**

This section pertains to the Cross Functional Services Framework. Cross Functional Services consist of the Plan, Build and Operate services that span across all the Service Frameworks. Cross Functional Services are composed of the following components: Security Management; Billing Management; Asset Management; Contract Management; Reporting; Disaster Recovery; Workflow; Capacity Management; Configuration Management; Account Management; Project Management, Quality Assurance; and Transition Services.

Cross Functional Services include IT lifecycle services that Contractor will provide across the County IT Service Frameworks. All requirements, roles and responsibilities described in this Schedule are considered to be within the scope of each IT Service Framework

### **7.2 Cross Functional Services High Level Requirements**

7.2.1 Contractor shall ensure that IT life cycle and service management functions are included in all IT Service Frameworks

7.2.2 Contractor shall provide IT services that consider an end-to-end enterprise view across all IT Service Frameworks

7.2.3 Contractor shall implement industry best practices process, quality, and project methodologies to align processes to people and technology to fulfill the County's mission.

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

7.2.5 Contractor shall monitor technical trends through independent research; document and report on products and services with potential use for the County.

7.2.6 Contractor shall provide the County insight into future direction, initiatives, and technology road maps of major applications vendors.

7.2.7 Contractor shall provide county government applications software and business experience and expertise – at the enterprise, business group, and departmental levels – to support Applications portfolio planning and strategic planning.

### 7.3 Security Management Services

#### 7.3.1 Security Management Services Overview

This section pertains to the Security Management Services component within the Cross Functional Framework. Security Management Services consist of the Plan, Build and Operate services that manage and enforce County security policies

#### 7.3.2 Security Management Services High Level Requirements

7.3.2.1 Contractor shall provide a phased consolidation, centralization, and standardization of security services employing a full-time, redundant set of systems, centralized management and awareness program using an available broadcast medium (e.g., network log-on messages, e-mail lists and help desk on hold recordings) that will lower the County's IT environment security cost.

7.3.2.2 Contractor shall provide the Services and process County Data using the best commercially-available security technologies and methods that meet or exceed requirements within the County Security Policy.

7.3.2.3 Contractor's security services shall include providing a central security organization, performing all necessary security assessments, providing a security plan that conforms to the requirements of local, State, and federal security laws and regulations, developing and maintaining a County-wide security policy and architecture, and performing all necessary security-related audits and reports.

7.3.2.4 Contractor shall provide physical security for all facilities under its management, security awareness and training programs, and operational support of system security processes for the Services.

7.3.2.5 Contractor will design and implement a centralized security system architecture that will facilitate tracking using an online Security Dashboard accessible to the County via a portal. The centralized system shall include:

- Centralized logging, auditing of system event logs and system configurations
- Intrusion detection and prevention
- Perimeter firewall management
- LAN isolation technologies

- Centralized user authentication and authorization services
- Vulnerability assessment
- Security incident tracking and response
- Reporting management that supports policy compliance detection, enforcement, and quick issue and incident remediation
- Periodic network scans and penetration test

**7.3.3 Security Management Services Requirements, Roles and Responsibilities**

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

<b>Security Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Define County requirements at the enterprise level for all security services (e.g. business, technology strategy, functional, availability, capacity, performance, applications, backup and IT continuity service)		X
2. Produce and submit quarterly updates to security requirements, standards, procedures and policies including regulatory requirements for County approval	X	
3. Review and approve security requirements, standards, procedures and policies for County		X
4. Produce and submit security architecture plans and requirements	X	
5. Review and approve security architecture plans and requirements		X
6. Produce and submit security violation reporting criteria	X	
7. Review and approve security violation report criteria		X
8. Review all security patches relevant to the IT environment and classify the need and speed in which the security patches should be installed	X	
9. Continuously monitor security trends through independent research; document and report on products and services with potential use for County as it aligns with County business and technology strategy	X	
10. Perform feasibility studies for the implementation of new security technologies that best meet County business needs and meet cost, performance and quality objectives	X	
11. Participate in technical and business planning sessions to establish security standards, architecture and project initiatives	X	
12. Conduct technical reviews and provide recommendations for improvements to the infrastructure that increase efficiency and effectiveness of security and reduce costs	X	
13. Establish and maintain list of authorized personnel who may initiate requests to Contractor focal point for off-site tape services		X

**Schedule 4.3 – Operational Services**

<b>Security Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
14. Produce and submit operational policies and procedures for Security Management	X	
15. Review and approve operational policies and procedures for Security Management		X
16. Implement appropriate controls within individual departments which recognize unique privacy issues that must be addressed and safeguarded to insure that individual departmental requirements are met (e.g. HIPAA, HHS, etc.)	X	
17. Alert the County to security patches that application software vendors recommend for rapid deployment under tested processes and procedures.	X	
18. Produce and submit Security Management testing and vulnerability analysis plan on a yearly basis	X	
19. Review and approve Security Management testing and vulnerability analysis plan on a yearly basis		X
20. Produce and submit policies and procedures for voicemail security	X	
21. Review and approve policies and procedures for voicemail security		X
22. Perform Application security planning for development and integration tasks	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
23. Implement and report results on security management testing and vulnerability analysis	X	
24. Review results security management testing and vulnerability analysis		X
25. Implement operational policies and procedures for security management	X	
26. Design, test and implement approved security architecture	X	
27. Identify relevant and applicable standards and methods to apply to County systems and applications to meet all special statutory and regulatory objectives and requirements	X	
28. Comply with all statutory requirements regarding systems, including specific regulatory requirements for systems affiliated with the California Law Enforcement Telecommunications System (CLETS) and the FBI Criminal Justice Information Systems (CJIS).	X	
29. Evaluate risk reduction and cost effectiveness of security processes and procedures		X
30. Implement test, evaluation, and re-test methods to prove that implemented security processes and procedures are working as planned	X	
31. Conduct integration and security testing for all new and upgraded equipment, networks, software or services to include unit, system, integration and regression testing	X	
32. Review all security patches relevant to the IT environment and classify the need and speed in which the security patches should be installed	X	
33. Maintain all documentation required for security audits and internal control and control testing	X	
34. Implement encryption technologies, security monitoring, anti-virus programs and relevant patches and upgrades as required by County policies and standards	X	
35. Design and implement an enterprise-wide virus management program that is integrated with the Help Desk, including centralized logging, signature	X	

**Schedule 4.3 – Operational Services**

<b>Security Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
distribution, patch distribution, client control and anti-virus event logging and signature distribution		
36. Design and implement a web-based security dashboard that will display meaningful metrics, aggregated security log data, and enable total IT security awareness of the County’s IT security environment	X	
37. Provide information from various frameworks into a central security monitoring system.	X	
38. Provide continuous monitoring, automated alerts, and notifications of virus removals, quarantines, and unknown exceptions and provide the County online access	X	
39. Develop and recommend improvement plans for County facilities as needed to maintain effective physical security	X	
40. Review and approve physical security improvement plans for County facilities		X
41. Implement physical and logical security measures consistent with County security requirements and industry standards (e.g., ISO 17799)	X	
42. Develop and document technical design plans and environment configuration based on County security requirements	X	
43. Review and approve all adjustments to County security policies, regulations and procedures as a result of new service features and components		X
44. Install and configure management tools in such a fashion that security problems, issues and events are proactively identified, reported and resolved	X	
45. Implement preventive measures for proactive monitoring and self-healing capabilities to limit outages due to security breaches that impact service delivery	X	
46. Develop and document security awareness and training programs in conformance with County security requirements	X	
47. Review and approve security awareness training		X
48. Design and implement voicemail security policies and procedures	X	
49. Produce and submit documentation to support Application designs which shall take into consideration County security policies	X	
50. Review and approve documentation to support Application designs for security considerations		X
51. Produce and submit System and Application security procedures	X	
52. Review and approve System and Application security procedures		X
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
53. Perform System access control according to approved policies and procedures	X	
54. Conduct security assessments and report monthly on vulnerabilities and recommended mitigations	X	
55. Maintain systems with specialized security requirements (e.g., Juris, CLETS). The CLETS system security shall be maintained by Contractor with oversight by Sheriff as set forth in Exhibit 12.1.1-1	X	
56. Produce and submit a listing of personnel that have been granted electronic access to County data/Systems maintained by the Contractor	X	
57. Provide and support security analysis and monitoring products into the	X	

**Schedule 4.3 – Operational Services**

<b>Security Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
County's system and network infrastructure		
58. Activate a security incident response team to respond to security events, and report events to appropriate security personnel	X	
59. Identify and track database security issues	X	
60. Resolve and report internal security violations	X	
61. Review and approve internal security violation resolution measures		X
62. Resolve and report security violations that originate outside of the hosted network(s) (e.g., denial of service attacks, spoofing, Web exploits)	X	
63. Perform security audits of desktops, servers, networks, and applications on a continuous, rolling basis, using monitoring tools such as network traffic analyzers (e.g. ethereal, etherpeek), network device monitoring (e.g. HP OpenView), device discovery services (e.g. nessus, nmap), and client configuration control agents (e.g. SMS)	X	
64. Conduct scheduled audit review meetings between the Contractor's security officer and the County security officer and related security working group(s)	X	
65. Scan network ports with standard scanning tools (e.g., nessus), with plug-ins included for scanning of known vulnerabilities of COTS application products	X	
66. Review and report unencrypted data transmissions vulnerable to network sniffing and interception	X	
67. Support County requested third party security audits, vulnerability and penetration testing	X	
68. Implement process for automated notification of transfers and termination of End-users	X	
69. Implement on-line access request process to request and authorize End-user IDs	X	
70. Ensure security of offsite storage for designated media and transport to and from offsite location as required	X	
71. Manage secure file transfers and other secure data movement activities	X	
72. Provide County with a detailed explanation of outages due to security breaches that identify the regional impact, source of breach, and preventative measures being taken to prevent future similar breaches and outages	X	
73. Act as a liaison to County Information Security Working Group (CISWG)	X	
74. Support periodic audits of security practices, process and procedures as required by County	X	
75. Submit authorized End-user list for County portfolio Applications		X
76. Deploy County portfolio Applications based on submitted authorized End-user list	X	
77. Provide security administration, including managing role and end-user database permissions	X	
78. Review the County's security policies annually and work with the County security officer to recommend updates, additions, or changes as the County's working IT environment changes	X	
79. Provide in-depth security training as part of optional training offerings	X	

7.4 Billing Management Services

7.4.1 Billing Management Services Overview

Billing Management services allow the County to accurately chargeback its internal business units for actual usage of IT resources and to receive accurate invoices that meet County requirements.

7.4.2 Billing Management Services High Level Requirements

7.4.2.1 Contractor will provide accurate and timely invoices with an appropriate level of detail for County requirements

7.4.2.2 Contractor will generate electronic billing information that facilitates the County’s chargeback activities

7.4.2.3 Contractor will support all activities required to audit, validate, substantiate, and detail its billings

7.4.2.4 Contractor shall enable rapid generation of timely reports and improve accuracy by eliminating the need for manual manipulation or transcription of raw data

7.4.3 Billing Management: Plan, Build and Operate Requirements, Roles and Responsibilities

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

<b>Billing Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Identify chargeback and reporting requirements		X
2. Identify monthly invoicing requirements		X
3. Produce and submit recommended monthly invoice/billing report format in accordance with County requirements	X	
4. Review and approve monthly billing report format		X
5. Document and maintain invoicing requirements	X	
6. Participate in, and support, billing audits as requested by the County	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Provide an automated interface with the County’s finance system for billing Services	X	

**Schedule 4.3 – Operational Services**

<b>Billing Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
8. Provide an automated interface with the County’s chargeback system in accordance with County requirements, including the ability for the County to review the chargeback reports and supporting data online through a Portal without any delays	X	
9. Produce and submit monthly reports (both hardcopy and electronically) detailing all usage and charges	X	
10. Maintain an electronic repository of all Billing Management records (reports, invoices, chargeback, etc.) for the duration of the contract	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Produce and submit to County chargeback reports and monthly invoices	X	
12. On a monthly basis, meet with the County’s finance staff to review invoices including: <ul style="list-style-type: none"> <li>○ Provide a mock invoice for review and agreement</li> <li>○ If discrepancies are identified, clarify and resolve them</li> <li>○ Meet again within a week to reach agreement on the changes or clarifications so the submitted invoice can be signed off</li> </ul>	X	
13. Approve chargeback reports		X
14. Download on a monthly basis all usage and charge information to the County chargeback application	X	
15. Provide invoices per County requirements	X	
16. Document and maintain County chargeback reporting requirements	X	
17. Calculate, report, and chargeback all applicable taxes and provide monthly billing for current and past services as well as track payments and balances	X	
18. Provide the billing data needed to reconcile bills	X	
19. Approve invoices		X
20. Maintain and provide an electronic archive of all billing and its details	X	

7.5 Asset Management Services

7.5.1 Asset Management Services Overview

Asset Management services are the activities associated with the asset tracking, pricing, evaluation (technical and costing), selection, acquisition, software license management and ongoing management of new and upgraded service components (e.g. hardware, software, circuits).

7.5.2 Asset Management Services High Level Requirements

7.5.2.1 Contractor will acquire and provision all assets required to perform the Services

7.5.2.2 Contractor shall provide an integrated requisitioning, sourcing, purchasing, and asset tracking system

7.5.2.3 Contractor will monitor, track, and provide timely reporting on assets throughout their life cycle and provide the County full visibility (e.g., asset, relevant accounting details, other by the contract information required)

7.5.2.4 Contractor will ensure inventory of assets is maintained and accurate

7.5.2.5 Contractor will manage all assets, including, but not limited to, ensuring that all assets are appropriately licensed

7.5.2.6 Contractor will provide Asset Management reports including Software (Desktop Applications Directory and Applications Portfolio) License Compliance, Application and Infrastructure Servers and Personal Computing Assets.

7.5.2.7 Contractor will work with 3<sup>rd</sup>-party vendors to optimize the pricing and terms for all 3<sup>rd</sup>-party assets

7.5.3 Asset Management Services Requirements, Roles and Responsibilities

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

<b>Asset Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommended asset management monthly report format (e.g., end-user name, department, account code, location, low-org)	X	
2. Review and approve asset management monthly report format		X

**Schedule 4.3 – Operational Services**

<b>Asset Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
3. Produce and submit recommended Software license monthly report format	X	
4. Review and approve recommended Software license monthly report format		X
5. Produce and submit asset management policies and procedures	X	
6. Review and approve asset management policies and procedures		X
7. Produce and submit Software license management policies and procedures	X	
8. Review and approve Software license management policies and procedures		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Implement asset management policies and procedures	X	
10. Implement Software License management policies and procedures	X	
11. Implement Software License monthly report	X	
12. Implement asset management monthly report	X	
13. Provide acquisition and tracking capability as required to fulfill County requests.	X	
14. Negotiate, enter into, track and manage all contracts, including licenses, with third-parties as required for the provision of the Services	X	
15. Provide and support an electronic Asset Management system which will include asset auto discovery tools to maintain asset data and user profiles	X	
16. Provide and support an electronic interface to the County's finance and chargeback systems to meet accounting, tracking, and reporting requirements	X	
17. Develop and implement on line access to Asset Management information	X	
18. Implement and support interfaces to feed asset location and financial data, including third party data such as relevant taxation, book and depreciation value data to an online reporting dashboard	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
19. Track and manage all assets provided by the Contractor	X	
20. Conduct periodic audits and provide exception reports resulting from use of asset auto discovery tools	X	
21. Produce and submit monthly reports on assets (both hardcopy and electronically)	X	
22. Produce and submit copies of all third-party contracts, including licenses, upon request of the County	X	
23. Produce and submit monthly software license management report	X	
24. Review and approve monthly software license management report		X
25. Validate compliance with applicable software licensing agreements using automated software tools and manual processes as required	X	
26. Verify installed software for non-networked PCs (that periodically touch the network to check e-mail, for example), while those PCs are in contact with the network.	X	
27. Report any license compliance issues no more than 30 days from the date of the issue	X	

<b>Asset Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
28. Report on contract expirations, license changes/upgrades, etc. in advance to prevent disruptions in service, non-compliance issues, etc.	X	
29. Report any expiration or renewal requirements for assets to allow for planning and mitigation	X	
30. Manage the ordering, procurement and delivery processes in compliance with County procurement and acceptance processes	X	
31. Maintain version control on asset inventory	X	
32. Dispose of assets (e.g. donation, sale, disposal) per County policies and procedures and accounting and financial requirements	X	

7.6 Contract Management Services

7.6.1 Contract Management Services Overview

Contract Management services are the activities associated with the ongoing management of the Agreement and the Contractor’s relationship with the County

7.6.2 Contract Management Services High Level Requirements

7.6.2.1 Contractor will interface, communicate and work with the County to ensure performance of the Agreement.

7.6.2.2 Contractor will assign a full-time contract/subcontract manager to contract to act as the single point of contact for the County on all contractual matters

7.6.3 Contract Management Services Requirements, Roles and Responsibilities

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

<b>Contract Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit Contract Management policies and procedures	X	
2. Review and approve Contract Management policies and procedures		X
3. Produce and submit an overall Application Services measurement plan to complement the MASLs, at no additional charge to the County. The measurement plan will collect key metrics to enable the County and the Contractor to identify productivity gains, better manage the services, and provide information for continuous improvement.	X	
4. Review and approve Application Services measurement plan		X
5. Produce and submit a high-level business case and cost estimate and present them for approval and funding when there is a probability that a package upgrade could provide considerable value to the County	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
6. Implement Contract Management policies and procedures	X	

**Schedule 4.3 – Operational Services**

<b>Contract Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
7. Support Contract Management policies and procedures	X	
8. Produce and submit a weekly program status report	X	
9. Produce and submit a monthly program status report	X	
10. Conduct monthly program status reviews with the County to include providing status on the Contractor’s achievement of the contractual objectives and to receive feedback	X	
11. Conduct quarterly reviews of adherence to standards and compliance with the County policies and schedules	X	
12. Produce and submit descriptions of contract issues and/or recommended contract change orders	X	
13. Review and approve contract change orders		X
14. Present monthly executive summary of performance to the County’s CIO and senior managers to include status, specific issues, recommended solutions and a view of planned activities.	X	
15. Provide program performance metrics electronically and in hard copy to designated County staff members	X	
16. Provide the County with weekly status updates to apprise relevant parties on the status of backlogged work requests and expected resolution dates	X	
17. Assist in planning technology transformation, projects, and equipment replacement to minimize the impact on the County’s yearly operations budget	X	
18. Manage relationship contact points with support partners and third-party providers to deliver a single POC for the processing and resolution of applications issues and problems	X	
19. Assist the County in evaluating actual performance versus budget by providing timely cost data, including: <ul style="list-style-type: none"> <li>▪ Assist the County in developing and executing routine reports that will allow insight into costs associated with the contract.</li> <li>▪ Assist the County to determine if chargeback allocations to business groups are correct and to make adjustment to the allocations if necessary</li> </ul>	X	
20. Assist the County in the development of their yearly operation budget by providing: <ul style="list-style-type: none"> <li>▪ Current, detailed, and accurate information relating to past operations</li> <li>▪ Assistance in costing and balancing the implementation of major initiatives</li> <li>▪ Assistance in spreading the costs of these major initiatives over multiple budget cycles</li> <li>▪ Technical support to determine the impact of changes in technology on costs.</li> <li>▪ Analysis of capacity use and performance</li> <li>▪ Identification of technical solutions for the reduction of operational costs</li> </ul>	X	
21. Produce and submit updates to the County Standards and Procedures Manual	X	
22. Review and approve updates to the County Standards and Procedures Manual		X

**7.7 Reporting Management Services**

**7.7.1 Reporting Management Services Overview**

Reporting services are the activities associated with the production and submission of designated reports and deliverables as described in this SOW, the MASLs and Schedule 5 of the Agreement. In addition, Contractor shall report system management information (e.g., performance metrics, and System accounting information) to the County.

**7.7.2 Reporting Management Services High Level Requirements**

7.7.2.1 Contractor will provide accurate and timely reporting on performance, trends, issues, assets, and other topics as required by the County

7.7.2.2 Contractor will proactively work with the County to ensure that all reports and deliverables are comprehensive and formatted to meet County requirements

7.7.2.3 Contractor will ensure that all reports are available to the County in both hardcopy and electronic formats

**7.7.3 Reporting Management Services Requirements, Roles and Responsibilities**

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

<b>Reporting: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Define reporting requirements, format and frequency		X
2. Assist the County to identify recurring reporting and format requirements to support the County’s needs for information	X	
3. Produce and submit Reporting operational policies and procedures based on County requirements	X	
4. Review and approve Reporting operational policies and procedures based on County requirements		X
5. Produce and submit recommendations for measurement and reporting of MASLs	X	
6. Review and approve recommendations for measurement and reporting of MASLs		X
7. Produce and submit required County reports	X	
8. Review and approve required County reports		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Design and implement required County reports	X	
10. Design and implement approved recommendations for measurement and reporting of MASLs	X	

**Schedule 4.3 – Operational Services**

<b>Reporting: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
11. Implement Reporting operational policies and procedures	X	
12. Design and implement an automated notification system that periodically reminds the report owner of upcoming submission dates. A summary of reports due within 30, 60, and 90 days will also be provided	X	
13. Design and implement a secure portal that will provide the County access to web-based, self-service, personalized customer displays of key IT and telecommunications management information	X	
14. Design and implement an automated data collection and reporting system that will support the County of San Diego’s yearly budgeting process, and give the County insight into the cost details of yearly operations	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
15. Produce and submit all reports and other written deliverables specified in Schedule 5 or Schedule 4.3	X	
16. Review and approve all reports and other written deliverables specified in Schedule 5 or Schedule 4.3		X
17. Provide the County access and input capabilities to Break-Fix incident and Problem tracking system to allow for Break-Fix incident/Problem monitoring and ad hoc reporting	X	
18. Provide status report detailing the root cause of and procedure for correcting recurring Problems and applicable Break-Fix incidents until closure as determined by the County	X	
19. Provide management reports to County on the progress of the all refresh plans	X	
20. Report on service performance improvement results	X	
21. Provide County configuration management reports	X	
22. Measure and Report monthly on each MASL	X	
23. Produce and submit monthly reporting on Applications, showing costs broken down by Plan, Build and Operate. The Operate costs should be broken down into the categories unscheduled maintenance, scheduled maintenance, administration, user support, and development and integration	X	
24. Produce and submit trend information on defects, Work Requests and estimate accuracy	X	

## 7.8 Disaster Recovery Management Services

### 7.8.1 Disaster Recovery Management Services Overview

This section pertains to the Disaster Recovery (DR) component within the Cross Functional Framework. The Disaster Recovery (DR) Services component encompasses all services, assets and facilities required to meet County requirements for Disaster Recovery (DR). The recovery time objectives (RTO) that shall be met by the Contractor are 48 hours for Priority 1 Applications and 72 hours for Priority 2 Applications. Application processing capability shall be restored within these timeframes, and restored data shall be no older than 28 hours prior to the disaster. In order to meet RTO, production application processing shall be split between the two Data Centers.

Contractor shall provide the County a complete disaster recovery plan, for the County's review and approval, to ensure the continuing availability of the Services during any event that would, under the circumstances, otherwise affect Contractor's ability to deliver the Services. The County may (at any time, and from time to time) identify and notify the Contractor in writing of other items, in addition to those described herein, that the County deems appropriate for inclusion in the disaster recovery plan. The Contractor shall promptly review and discuss with the County all such additional items and, unless the County agrees otherwise in writing, promptly revise the disaster recovery plan to properly address such additional items. In addition, prior to each anniversary of the first Cutover Date, the Contractor shall revise the disaster recovery plan as appropriate to reflect any changes to the County's IT environment, or related requirements, and submit such revised disaster recovery plan to the County for review, comment, and approval. Commencing not later than on the Cutover Date for each Service Framework, Contractor shall implement the plan and provide the County disaster recovery services so as to ensure the continuing availability of all Services related to such Service Framework.

### 7.8.2 Disaster Recovery Management Services High Level Requirements

- 7.8.2.1 Promote disaster recovery and business continuity (BC) at the County in the event of a disaster
- 7.8.2.2 Provide recovery and resumption of County Priority 1 Applications, as defined in MASL Break-Fix, within 48 hours
- 7.8.2.3 Provide recovery and resumption of County Priority 2 Applications, as defined in MASL Break-Fix, within 72 hours.

**Schedule 4.3 – Operational Services**

7.8.2.4 Prevent data loss of no greater than 28 hours

7.8.2.5 Test DR preparedness on a yearly basis to ensure readiness

**7.8.3 Disaster Recovery Management Services Environment**

**7.8.3.1 Contractor Facilities**

The DR Services will be performed across both active Contractor Data Centers, and other facilities as required.

**7.8.4 Disaster Recovery Management Services Requirements, Roles and Responsibilities**

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

<b>Disaster Recovery Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit a Disaster Recovery (DR) plan that meet County requirements	X	
2. Review and approve a DR plan that meet County requirements		X
3. Produce and submit data recovery plan consistent with the County’s business requirements	X	
4. Review and approve data recovery plan		X
5. Produce and submit at the start of each Contract Year a revised DR Plan to continually meet County objectives	X	
6. Review and approve the yearly DR Plan		X
7. Produce and submit a yearly DR test plan	X	
8. Approve the DR/BC test		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Design and implement DR plan	X	
10. Design and implement data recovery plan	X	
11. Coordinate the DR plans with group Business Continuity (BC) plans to address any potential disconnects or misunderstanding	X	
12. Perform yearly DR test	X	
13. Submit yearly DR test results to the County	X	
14. Review and approve yearly DR test results		X
15. Maintain and document requirements for off-site data storage	X	
16. Review documentation for off-site data storage		X

**Schedule 4.3 – Operational Services**

<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
17. Provide secure offsite storage for designated media and transport media to offsite location as required (include handling, storing, shipping, and receiving tape media) – transport tapes in environmentally controlled vehicles operated by bonded personnel. The off-site facility will have complete fire protection and multiple layers of physical security to prevent unauthorized access	X	
18. Ensure archived data is available for use in disaster recovery operations	X	
19. Provide off-site backup media storage	X	
20. Establish and maintain contracts for hot-site or cold-site availability as required, coordinate disaster recovery exercises to ensure readiness, and perform required recovery	X	
21. Promote DR and use of BC by meeting with the County’s CIO, IT governance committees, the business managers, and the departments to provide appropriate communication during any DR operation	X	
22. Perform scheduled DR tests per County policies, requirements and the DR Plan	X	
23. Track and report DR test results to the County	X	
24. Approve DR testing results		X
25. Perform corrective action identified during the DR test and provide ongoing status until completion	X	
26. Provide a written DR test and corrective action report to the County by a mutually agreed upon date each year	X	
27. Execute DR Procedures when directed by an authorized representative of the County	X	
28. Provide DR recovery within 48 hours from the time a disaster is declared for Priority 1 Applications	X	
29. Provide DR recovery within 72 hours from the time a disaster is declared for Priority 2 Applications	X	

7.9 Workflow Management Services

7.9.1 Workflow Management Services Overview

Workflow Services encompass all of the systems and services required to: process requests for service from the County; coordinate Contractor activities to provide the Services; and coordinate with 3<sup>rd</sup>-parties as required to provide the Services.

7.9.2 Workflow Management Services High Level Requirements

7.9.2.1 Contractor will provide efficient and effective processing of County requests for service

7.9.2.2 Contractor will work with the County to develop and implement workflow policies and procedures that provide appropriate efficiency, security, and control

7.9.2.3 Contractor will link processes by automating functions using a common toolset and a framework of IT Infrastructure Library (ITIL) -based integrated processes

7.9.2.4 Contractor will coordinate its own, Subcontractor, and 3<sup>rd</sup>-party resources to provide high-quality services

7.9.2.5 Contractor will provide access to County end-users and management on the status (both current and historical) of requests for service

7.9.3 Workflow Management Services Requirements, Roles and Responsibilities

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

<b>Workflow Management Services : Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for Workflow operational policies and procedures	X	
2. Review and approve recommendations for Workflow operational policies and procedures		X
3. Produce and submit closed loop methodology for Workflow entry, tracking and closing of the Work Request	X	
4. Review and approve closed loop methodology for Workflow entry, tracking and closing of the Work Request		X
5. Produce and submit recommended monthly report format for requests for service	X	

**Schedule 4.3 – Operational Services**

6. Review and approve monthly report format for requests for service		X
7. Produce and submit monthly reports detailing all requests for service (both hardcopy and electronically)	X	
8. Approve Break-Fix and Problem management policies and procedures		X
9. Produce and submit escalation/notification policies and procedures	X	
10. Review and approve escalation/notification policies and procedures		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Design and implement closed loop methodology for Workflow entry, tracking and closing of the Work Request	X	
12. Implement approved Workflow operational policies and procedures	X	
13. Implement monthly reporting	X	
14. Implement and maintain a service ordering process that clearly defines how to order, change or delete Services	X	
15. Establish and implement adequate Break-Fix Incident/Problem Ticketing, tracking, workflow, escalation, communication and reporting processes to ensure the MASL and other County requirements are met	X	
16. Ensure Break-Fix Incident resolution activities conform to defined change control procedures	X	
17. Perform integration tasks for all System Break-Fix incidents	X	
18. Develop and execute procedures for conducting End-user satisfaction surveys according to MASLs and Schedule 7.2 (End User Satisfaction Surveys	X	
19. Review and approve procedures for conducting End-user satisfaction surveys		X
20. Escalate and resolve issues with development, integration and service delivery teams	X	
21. Implement escalation/notification policies and procedures	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
22. Ensure that all questions, Help Desk requests, and Work Requests are routed to the appropriate parties for timely resolution	X	
23. Provide status, upon request of the County, of all questions, Help Desk requests, and Work Requests	X	
24. Ensure applicable Work Requests are properly authorized	X	
25. Manage entire Break-Fix Incident/Problem lifecycle including detection, diagnosis, County status reporting, repair and recovery	X	
26. Provide notice to affected End-users of any service interruptions to allow County planning and mitigation	X	
27. Participate in Problem review sessions and provide listing and status of Problems categorized by Problem impact	X	
28. Authorize closure of all Work Requests		X
29. Manage efficient workflow of Break-Fix incidents including the involvement of third party providers (e.g., vendors, public carriers)	X	
30. Categorize Break-Fix incident/Problem classification by priority	X	
31. Process all Work Requests	X	

**Schedule 4.3 – Operational Services**

32. Produce and submit to County Break-Fix Incident and Problem management policies and procedures	X	
33. Support escalation/notification policies and procedures	X	

7.10 Capacity and Performance Management Services

7.10.1 Capacity and Performance Management Services Overview

Capacity and Performance Management services include all systems and services relating to optimizing the efficiency, effectiveness, and performance of the County’s systems.

7.10.2 Capacity and Performance Management Services High Level Requirements

7.10.2.1 Contractor will monitor and manage systems to leverage and optimize the County’s IT investment

7.10.2.2 Analyze historical resource usage of tracking and trending by CPU, memory, input/output, and storage

7.10.2.3 Contractor will monitor system use and capacity by analyzing historical resource use trends for the 12 prior months and forecast short-term and long-term infrastructure resource usage and performance

7.10.2.4 Contractor will identify and implement improvements to better leverage existing capacity

7.10.2.5 Contractor will communicate potential capacity or performance issues to the County in advance, and implement approved solutions in a timely manner

7.10.3 Capacity and Performance Management Services Requirements, Roles and Responsibilities

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

<b>Capacity and Performance Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Conduct capacity planning activities that incorporate all Systems, sub-systems, and software, workload balancing, and resource allocation	X	
2. Recommend changes to capacity to improve service performance	X	
3. Approve capacity related recommendations		X
4. Produce and submit recommendations for changes to optimize capacity management	X	

*Schedule 4.3 – Operational Services*

<b>Capacity and Performance Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
5. Review and approve changes to optimize capacity management	X	
6. Produce and submit projections prior to the beginning of each contract year regarding estimated usage and loading for all Service Frameworks based on historical trends, anticipated new projects and decommissioning of systems, etc.	X	
7. Develop and maintain a capacity plan to meet the County’s existing and future needs. The process components of the capacity Management plan shall include: <ul style="list-style-type: none"> <li>▪ Application sizing</li> <li>▪ Resource forecasting</li> <li>▪ Demand forecasting</li> <li>▪ Modeling</li> <li>▪ Performance monitoring</li> <li>▪ Workload monitoring</li> </ul>	X	
8. Perform Application capacity and performance planning, incorporating business projections provided by the County	X	
9. Perform capacity and performance planning on an ongoing basis when new business and application growth is anticipated, when changes to existing business requirements are anticipated or occur, or when system configuration changes are performed	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
10. Implement comprehensive capacity management planning process	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
11. Maintain capacity levels to optimize use of existing IT resources and minimize County costs to deliver Services in accordance with the MASLs	X	
12. Monitor and manage capacity in all Service Frameworks to maximize performance and efficiency, and to minimize service disruptions	X	
13. Assess impact/risk and cost of capacity changes and submit mitigation recommendations	X	
14. Continually monitor IT resource usage to enable proactive identification of capacity and performance issues	X	
15. Capture trending information and forecast future County capacity requirements based on County defined thresholds	X	
16. Assess capacity impacts when adding, removing or modifying Applications	X	
17. Assess Break-Fixes and incidents/Problems related to throughput performance	X	
18. Recommend and perform approved DBMS tuning changes	X	
19. Conduct periodic database reorganizations as indicated by usage and performance	X	
20. Define and execute database performance and tuning scripts and keep database running at optimal performance for County’s workload	X	
21. Implement and administer appropriate database management tools across all database instances	X	

7.11 Configuration Management Services

7.11.1 Configuration Management Services Overview

Configuration Management services are the activities associated with the recording, tracking, updating and dissemination of County configurations for all hardware and software assets.

7.11.2 Configuration Management Services High Level Requirements

7.11.2.1 Contractor will monitor, optimize, maintain, document, and report on all County hardware and software configurations, including but not limited to new releases and versions, patches, and bug fixes.

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

7.11.2.3 Contractors will perform configuration identification, control, status accounting, audits and release management according to County policies and procedures

7.11.2.4 Contractor will standardize change management technologies for Service Frameworks as defined and approved by the County.

7.11.2.5 Contractor will maintain all hardware and software within one release of such hardware and software manufacturers’ latest release, unless otherwise approved by the County

7.11.3 Configuration Management Services Requirements, Roles and Responsibilities

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

<b>Configuration Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit configuration management policies, procedures and policies	X	
2. Review and approve configuration management policies, procedures and standards		X
3. Produce and submit recommendations for configuration changes	X	
4. Review and approve configuration changes		X

**Schedule 4.3 – Operational Services**

<b>Configuration Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
5. Monitor vendor announcements regarding software upgrades, patches, problems and published solutions, provide impact analysis and propose installation plans for announce fixes	X	
6. Recommend which applications packages should be regularly reviewed for patches or version release upgrades and review this list per a defined schedule	X	
7. Provide release and upgrade management per the following steps: <ul style="list-style-type: none"> <li>a. Determine vendor package classification, whether commercial-off-the-shelf, ERP, or third-party</li> <li>b. Review contractual obligations for application support from current application vendors</li> <li>c. Obtain certification and schedule of current release support</li> <li>d. Discuss integration with upcoming IT strategic initiatives</li> <li>e. Receive monthly input from the patch or upgrade management team for new release requirements and present the requirements to the County for approval and acceptance.</li> <li>f. Once the IT governance groups accept the business case and approve the strategy plan, consult the County for project planning and scheduling</li> </ul>	X	
8. Identify and report when patches or version-release upgrades are available for Applications and determine which functionalities are newly available as a result of the upgrade or which system issues are addressed by it, particularly when this improves customer ease of use	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
9. Implement and maintain configuration management policies and procedures	X	
10. Establish a Change and Release Control Board (CRCB) that will approve CM policies and their inclusion in standards and procedures in the County Standards and Procedures Manual, and will approve or delegate approval of changes and releases of updates	X	
11. Participate in Change and Release Control Board (CRCB) and review and approve CRCB activities and decisions		X
12. Select, install and maintain configuration management tools	X	
13. Ensure that change control and notification processes are followed for installations, upgrades and adjustments to components, software and County processes.	X	
14. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing	X	
15. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and regressing of configuration items	X	
16. Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states	X	
17. Establish process for verifying the accuracy of configuration items; adherence to configuration standards, management process and the identification of process deficiencies	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>

**Schedule 4.3 – Operational Services**

<b>Configuration Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
18. Perform configuration management	X	
19. Install manufacturer field change orders, service packs, firmware, and software maintenance releases, etc.	X	
20. Perform configuration management activities throughout the system life-cycle	X	
21. Perform configuration management activities throughout the development life cycle	X	
22. Perform configuration management and change management activities related to integration and testing	X	
23. Perform product patch, “bug fix,” service pack installation or upgrades to the current installed version	X	
24. Review configuration management results		X
25. Maintain master copies of new versions in a secured software library and update configuration databases	X	
26. Administer the version control system as it relates to release management of County Applications	X	
27. Ensure that inventory and configuration management records are maintained and that all updates to County and Contractor records are reflected	X	
28. Provide document version control for all documentation for which Contractor is responsible	X	
29. Inform the County of changes through the weekly change and release control meetings and periodic integrated change status reporting. Each change request shall identify other related change requests to facilitate integrated reporting.	X	

7.12 Account Management Services

7.12.1 Account Management Services Overview

Account Management services provide for the consolidation and simplification of account administration across the Service Frameworks for the County user.

7.12.2 Account Management Services High Level Requirements

7.12.2.1 Maintain a single point of contact via the Help Desk for all End-user account authentication and authorization activities including account creation, password reset, account deletion or data permission setting.

7.12.2.2 Implement and maintain a solution to synchronize accounts across the enterprise and across disparate systems for users. This uniformity will allow account management across the enterprise, enable administrators to synchronize accounts and passwords and to provide role-based provisioning

7.12.2.3 Reduce the number of End-user accounts a single End-user requires to access business applications

7.12.3 Account Management Services Requirements, Roles and Responsibilities

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

<b>Account Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommended processes for Account Management authentication and authorization	X	
2. Review and approve processes for Account Management authentication and authorization		X
3. Produce and submit escalation procedures for quick termination	X	
4. Review and approve escalation procedures for quick termination		X
5. Produce and submit End-user Account Management architecture	X	
6. Review and approve End-user Account Management architecture		X
7. Produce and submit End-user account consolidation plan	X	
8. Review and approve End-user account consolidation plan		X
9. Produce and submit the format for a report detailing all County End-user accounts and End-user data permissions	X	
10. Review and approve the format for a report detailing all County End-user accounts and End-user data permissions		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>

**Schedule 4.3 – Operational Services**

<b>Account Management: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
11. Implement systems to centrally manage and maintain Account Management datum and activities	X	
12. Implement approved processes for Account Management authentication and authorization	X	
13. Implement reports detailing all County End-user accounts and End-user data permissions	X	
14. Implement End-user account consolidation plan	X	
15. Analyze account management architecture and the access control systems of the County’s business applications, and develop and implement an End-user Account Consolidation Plan and End User Account Management Architecture that will provide a platform for account synchronization across the enterprise and across disparate systems	X	
16. Implement End-user Account Management Architecture	X	
17. Implement escalation procedures for quick termination	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
18. Centrally maintain End-user accounts	X	
19. Perform End-user account maintenance to include account creation, deletion or modification	X	
20. Perform End-user account password resets	X	
21. Perform End-user authorized data permission requests	X	
22. Facilitate the receipt and tracking of requests for End-user account activation, changes and terminations	X	
23. Facilitate the creation, change and deletion of End-user accounts	X	
24. Coordinate as necessary with other specialized areas to manage End-user accounts	X	
25. Maintain Access Control Lists (ACL) in accordance with policies	X	
26. Provide report detailing all County End-user accounts and End-user data permissions on a monthly basis	X	
27. Provide an auditable record of security modifications and produce reports and notifications of end-user access modifications, transfers, and terminations	X	
28. Provide support, including break-fix, for all Account Management services	X	
29. On an annual basis, update the End-user Account Consolidation Plan to reflect progress toward reduction of User IDs and credentials, and to make recommendations for implementation of new technologies within the Account Management Architecture	X	

7.13 Project Management Services

7.13.1 Project Management Services Overview

Project Management services include the provision of standardized and industry accepted methodologies for project planning, tracking, management and reporting for all Service Frameworks other than Applications Services.

7.13.2 Project Management Services High Level Requirements

7.13.2.1 Contractor will provide qualified program and project management resources with relevant background and experience including PMI certification

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

7.13.3 Project Management Services Requirements, Roles and Responsibilities

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

<b>Project Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit recommendations for standard project management tools, reports, and artifacts	X	
2. Review and approve standard project management tools, reports, and artifacts		X
3. Produce and submit recommendations for project-specific tools and artifacts	X	
4. Review and approve project-specific tools and artifacts		X
5. Produce and submit resource-loaded project plans for all projects	X	
6. Review and approve resource-loaded project plans for all projects		X
7. Produce and submit project status reports on no less than a monthly basis	X	
8. Provide a range of training options, including attendance at seminars, user groups, and vendor training		
9. Produce and submit project management policies and procedures	X	
10. Review and approve project management policies and procedures		X
11. Recommend business process reengineering methodologies	X	
12. Assess and approve business process re-engineering methodologies		X
13. Identify opportunities for business process improvements	X	
14. Provide industry knowledge applicable to County departmental business to identify opportunities for business process reengineering and Application development and integration/modification	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>

**Schedule 4.3 – Operational Services**

<b>Project Management Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
15. Implement County authorized Project Management discipline	X	
16. Work in conjunction with the County’s training and development resources to provide a common look and feel to training delivery methods	X	
17. Implement and manage County-authorized Project Management tools and processes based on industry standards and best practices	X	
18. Develop and maintain a training course catalog in cooperation with County HR and the business units to provide end users access to training so they can develop the necessary skills to fulfill their responsibilities	X	
19. Implement approved project management policies and procedures	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
20. Support project management policies and procedures	X	
21. Provide high quality project management for all initiatives and projects undertaken as part of the Services	X	
22. Participate in Program management and Project management activities as required to insure successful work efforts		X
23. Facilitate project status reviews with County management and staff on no less than a monthly basis	X	
24. Distribute the standard project processes, templates, or other vehicles, to all stakeholders to collect relevant project operational and performance data	X	
25. Support the County’s Verification & Validation activities including assisting in identifying errors, risk factors, omissions, discrepancies, constraints, performance and security problems, and other obstacles in project implementations	X	
26. Provide local venues for training, particularly for Cross-Functional Services training or special purpose training when delivering training to users in their environment is not practical (e.g., when providing training on new systems or applications for which a computer laboratory type environment is necessary and will be leveraged across many training sessions)	X	

7.14 Quality Assurance Services

7.14.1 Quality Assurance Services Overview

Quality Assurance (QA) Services include the systems and services required to ensure high quality performance of the Services. Quality Assurance Services will provide Plan, Build and Operate services for a Root Cause Analysis (RCA) process. The RCA process will diagnose, analyze, recommend, and take corrective measures to prevent recurring Problems and/or trends.

7.14.2 Quality Assurance Services High Level Requirements

7.14.2.1 Contractor will utilize oversight and assurance resources, policies, procedures, and other means to provide high-quality performance of the Services

7.14.2.2 Contractor shall deliver a Quality Assurance program that is compliant with the International Organization for Standardization (ISO) 9001-2000 quality model, Institute of Electrical and Electronics Engineers (IEEE) processes and standards, and Capability Maturity Model® Integration (CMMI) Level 3 standards.

7.14.2.3 Contractor will work collaboratively with the County to ensure the most efficient and effective use of QA resources and processes.

7.14.3 Quality Assurance Services Requirements, Roles and Responsibilities

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

<b>Quality Assurance Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit QA Services policies and procedures	X	
2. Review and approve QA Services policies and procedures		X
3. Produce and submit policies and procedures for Root Cause Analysis (RCA)	X	
4. Review and approve policies and procedures for Root Cause Analysis (RCA)		X
5. Produce and submit procedures for process improvement	X	
6. Review and approve procedures for process improvement		X
7. Keep informed of changing audit requirements and changes in laws that affect scripts and tools used to comply with them	X	
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
8. Implement QA Services policies and procedures	X	
9. Implement policies and procedures for Root Cause Analysis (RCA)	X	
10. Implement procedures for continuous process improvement based on best practices and industry standard methods for delivering IT service management	X	

**Schedule 4.3 – Operational Services**

<b>Quality Assurance Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
to optimize the County’s enterprise solution		
11. Implement a total quality management plan integrated with the quality assurance plan	X	
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
12. Perform internal QA activities to ensure a high-level of performance and quality in all Service Frameworks	X	
13. Audit Contractor Operations and Maintenance activities for compliance with Operational policies & procedures		X
14. Produce and submit results of internal audits (self-assessments) relating to the County’s service frameworks	X	
15. Review and approve internal audit findings (self-assessments)		X
16. Incorporate audit findings into County Service frameworks as necessary to maintain compliance	X	
17. Recommend resolutions to address recurring Problems or Failures	X	
18. Review and approve resolutions to address recurring Problems or Failures		X
19. Track and report recurring Problems or Failures and provide associated consequences of Problems if there is a business impact to the County	X	
20. Perform root cause analysis of Break-Fix incidents, document findings and take corrective actions for in scope services. Resolve Problem and/or substantiate that all actions have been taken to prevent future reoccurrence.	X	
21. Ensure that recurring Problems which meet defined criteria are reviewed using root cause analysis processes	X	
22. Routinely assess customer satisfaction at program and service element levels using automated survey tool	X	
23. Initiate additional survey processes as required to measure Contractor’s performance rating.		X
24. Report results and trend analysis of customer satisfaction surveys with corrective action plans, as needed, in the monthly status report	X	
25. Periodically audit selected functions to verify that established policies and procedures are being followed and, if variances are noted, recommend corrective actions.	X	
26. Perform periodic internal audits to check that standards are being followed.	X	

7.15 Transition Services

7.15.1 Transition Services Overview

Transition Services include the Plan, Build, and Operate activities required to transition the County successfully, in a timely manner with minimal operational impacts, to the Contractor’s facilities, resources, systems, and services.

7.15.2 Transition Services High Level Requirements

7.15.2.1 Contractor will leverage its experience in conducting transitions to develop complete and comprehensive transition plans with minimal risk (including contingency plans)

7.15.2.2 Contractor will provide appropriate facilities, resources, systems, and services to facilitate the transition of County Services with minimal operational impacts

7.15.3 Transition Services Requirements, Roles and Responsibilities

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

<b>Transition Services: Plan, Build and Operate Requirements, Roles and Responsibilities</b>		
<b>Plan Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
1. Produce and submit Transition Plan	X	
2. Review and approve Transition Plan		X
<b>Build Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
3. Implement approved Transition Plan	X	
4. Provide weekly status reports on Transition Plan execution	X	
5. Review weekly status reports on Transition Plan execution		X
<b>Operate Requirements, Roles and Responsibilities</b>	<b>Contractor</b>	<b>County</b>
6. Implement and support Transition Plan	X	
7. Perform Services in accordance with MASLs and transition MASLs.	X	
8. Coordinate and collaborate with third-party service providers to minimize service impacts and expedite the transition to Contractor Services	X	

7.16 Domain Names Management Services

7.16.1 Domain Names Management Services Overview

Domain Names Management Services include the activities required to successfully manage all County domain names in a centralized manner. The scope includes actively monitoring current subscriptions, renewing subscriptions and paying appropriate fees to domain name vendors.

#### 7.16.2 Domain Names Ownership

In order for Contractor to manage the domain names on behalf of the County, Contractor must assume ownership. As part of the one-time project, Contractor will work with County owners to transfer ownership of their domain names to Contractor's Domain Name Administrator. The One-Time Transfer Project Fee as defined in Schedule 16.1 – Fees, Section 21.1, covers transference of the County employee owned domain names as described therein. Transfer of County domains owned by individuals outside the County may be included at a time and materials basis, as approved by the County.

Once the One-Time Project is complete, if more domain names are discovered or purchased by the County, and the County wishes to add them to the Domain Name Management service, a Transference Fee as defined in Schedule 16.1 – Fees, Section 21.2 will be applied for each additional domain name.

#### 7.16.3 Portfolio of Domain Names

The Domain Names portfolio will be maintained by the Contractor Domain Name Administrator and include the following information:

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

#### 7.16.4 Domain Extensions

This Domain Names Management services will cover the following domain types:

- .biz
- .com

- .info
- .mobi
- .net
- .org
- .us

Additional extensions that are available through ordinary domain name registrars at the same cost range (+/- 20%) as those above may also be covered.

Only one site with extension .gov will be managed on behalf of the County as part of this service: “sdcounty.ca.gov”

#### 7.16.5 New Domain Name Process

County Point of Contact (POCs) may request a new domain name via the catalog process. This request will be considered authorization to purchase the name and add the domain to the portfolio, which will be charged through the Monthly Management Fee.

Per County requirements, the new domain name must conform to the then current County standards and the Contractor Domain Name Administrator will check for compliance. In the absence of published County standards, the requested name will be accepted by Contractor. If the standards are published and the requested name does not conform, the Contractor Administrator will request that the County POC selects a name that meets the County standards.

The Contractor Domain Name Administrator will determine through the registrar if the requested domain name is available. If it is, the purchase will be made, the domain added to the portfolio, and the County POC notified.

If the requested name is not available, the Contractor Domain Name Administrator will notify the County POC to select another name. Once an available name is selected, the Contractor Domain Name Administrator will purchase it, the domain will be added to the portfolio and the County POC notified.

Since new domain names are most frequently needed during applications projects, the County POCs may delegate the request process to Contractor project managers or other designates to perform as part of a work request.

#### 7.16.6 Renewal Process

At least 30 days prior to any domain name expiration, the Contractor Domain Name Administrator will notify the County POC of any upcoming renewal. Once the County POC approves the renewal, the purchase will be made and updates made to the domain name portfolio. If the domain name is no longer needed, the County POC may request not to renew the domain name. If so, the domain name will not be renewed and the domain will be retired from the portfolio.

Early cancellations of domain names outside the normal renewal cycle are not allowed.

#### 7.16.7 Reports

Contractor Domain Name Administrator will provide County POC with a monthly report containing the following information:

- Total quantity of domain names in the portfolio
- Quantity of new domain names added in the last month
- Quantity of domain names transferred in the last month
- Quantity of domain names retired in the last month
- Quantity of domain names retained by the County but removed from HP ownership in the last month
- Summary data for each domain name:
  - Domain name ID
  - Domain name
  - Type / Extension
  - Renewal Date
  - High Org
  - Low Org
  - County POC Name, Email and Phone
  - Secondary County POC Name, Email and Phone

### **8 Minimum Acceptable Service Levels (MASLs)**

Contractor shall, at a minimum, perform the Services in accordance with the MASLs. The MASLs are set forth in Exhibit 4.3.8 Minimum Acceptable Service Levels (MASLs).

### **9 Infrastructure Engineering Services**

#### 9.1 Infrastructure Engineering Services Overview

Contractor will provide Infrastructure Engineering services as requested by the County in accordance with the Infrastructure Engineering Services stipulated in Schedule 16.1 Fees Section 19.

**END OF SCHEDULE**