Deloitte.

State of Louisiana
Office of Information Technology

IT Consolidation

Operational Plan for Service Management and Delivery

Table of Contents

1.0 Introduction

This document describes the IT Operational Plan for the consolidated central IT organization for the State of Louisiana.

1.1 Operational Plan

The Operational Plan describes the proposed operational activities and processes for the central IT organization for the State of Louisiana. Many of the processes are not currently in place as of February 2014, but are proposed for the future state organization. The activities and processes are determined using the IT Operating Model framework described in the Operational Plan Approach section. The framework describes the processes and sub-processes to govern operations in the consolidated IT organization for the State of Louisiana.

The document then details each of the sub-processes that central IT should follow for optimal IT operations for the State of Louisiana"s systems.

1.2 Audience

The primary audience for this document is the State of Louisiana central IT management that operates State systems for participating departments. Other State employees involved in planning, approving, executing and overseeing agency programs and those in central IT that support these processes can also benefit from this document.

1.3 Scope

Each process and activity described in this document is not intended to be a detailed step-by-step guide to operate the State of Louisiana environments. Rather, the processes and activities described here are the standard processes that central IT should enact to operate the IT environments with standard processes and consistency of service delivery.

1.4 Document Organization

The document is organized as follows:

- **Section 1**: Introduction provides a brief description to the IT operational plan document.
- **Section 2**: Operational Plan Approach describes the IT Operating Model Framework, including its purpose and organization.
- **Section 3**: Operational Plan Processes details the processes and activities included in the IT Operating Model Framework for Technology and Infrastructure Management, Service Transition, Service Portfolio Management, and Service Operation.

2.0 Operational Plan Approach

The Operations Model framework shows the operational plan approach for the central IT environment for the State of Louisiana and the organization of activities into traditional Plan, Build, Transition and Run categories. The scope of the operations approach focuses on the areas in the black bold border including Transition, Run, and Technology/Infrastructure Management.

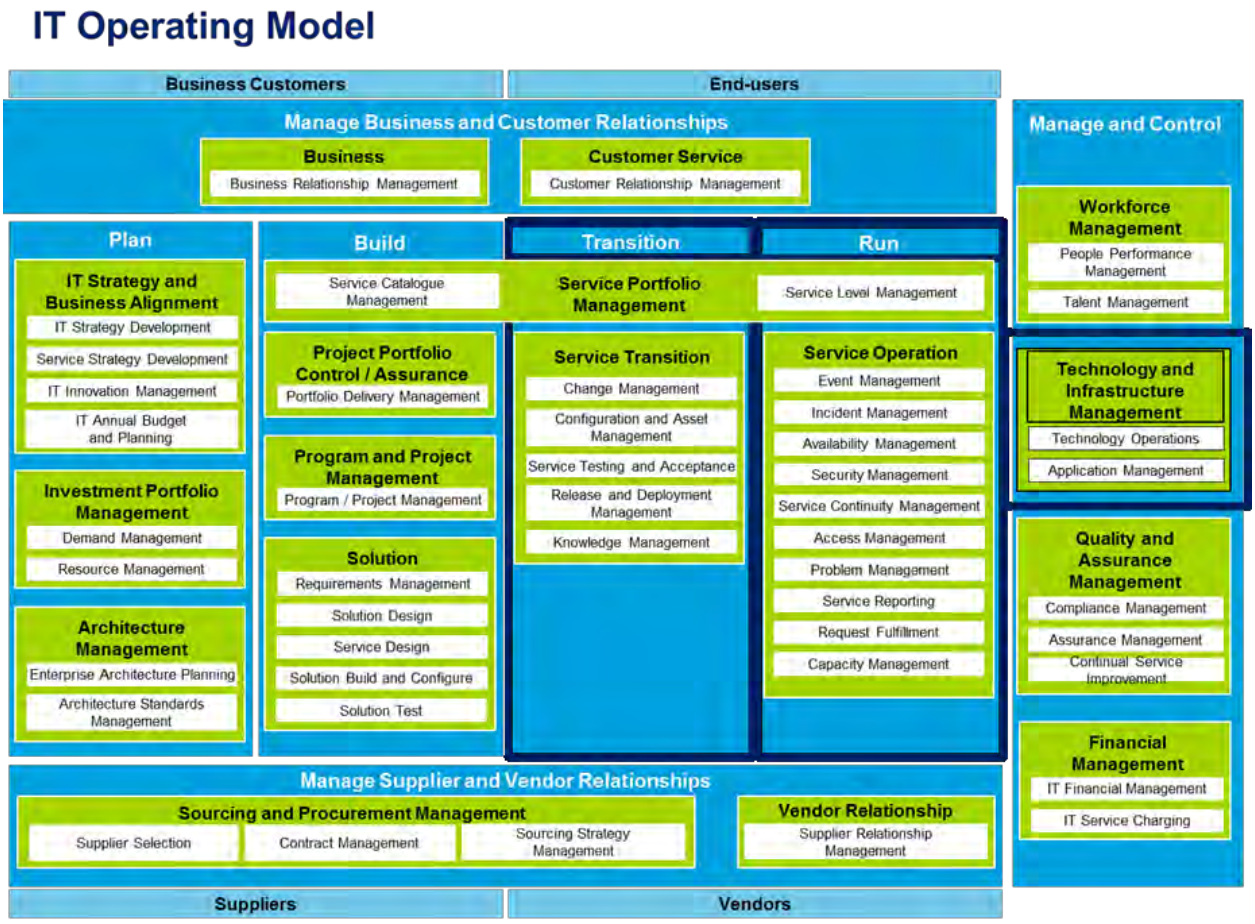

Figure 2.1.1 – IT Operational Plan Framework

2.1 Service Portfolio Management

Service Portfolio Management includes the development and maintenance of an IT Service Catalog and corresponding Service Level Agreements.

- **Service Catalog Management**: The central IT team will maintain an updated and current service catalog to keep customers abreast of all services provided by IT. The service catalog will be

available to all customers in an end-user friendly format. Standard processes and procedures will be followed to add, remove, and modify services to best align central IT and customer goals.

- **Service Level Management**: The central IT team will continually work to improve the services provided by tracking and monitoring service levels and working continuously to improve service delivery. Central IT will not only track industry standard service level metrics and key performance indicators to evaluate performance, but will also gain informal feedback through follow-up calls and management queries to identify ways to improve performance in the future.

2.2 Service Transition

For the Operations Approach, central IT will provide the services to aid in seamless transition of operations activities. These activities include:

- **Change Management**: Managing the change management process is typically one of the most challenging areas in operations support and central IT will provide the rigor and controls to make sure Change Management is handled according to the designed procedures. IT will develop and implement Change Management processes for standard changes as well as emergency changes to minimize risk of deployment and meet the needs of the agencies.
- **Configuration and Asset Management:** The central IT team will use a single service desk and change management tool to perform the Configuration and Asset Management activities. All IT assets within the architecture will be tracked and managed using the tool with any updates creating a configuration item (CI) that will update the Asset Management system. Any problems identified in the system will also create a configuration item to perform problem resolution.
- **Service Testing and Acceptance:** The central IT team will utilize standard processes and procedures for testing and accepting services. These processes will be closely aligned with the Change Management processes to make sure any changes implemented perform as expected and do not disrupt current operations. Regression testing is a critical function of Service Testing and the central IT team will develop and implement regression testing plans with every release.
- **Release and Deployment Management:** The central IT team will manage every release with care and planning to attempt to make sure every planned implementation goes smoothly. The central IT team will follow the release management process to make sure the approvals for the releases are acquired and the steps for successful introduction of updates to the current environment are completed according to plans.
- **Knowledge Management:** Central IT will maintain a current listing of knowledge articles to help end-users and central IT staff resolve incidents and utilize IT services more effectively. Central IT will use procedures to add articles to the knowledge base whenever a need for a new knowledge article is identified that is not currently documented. Having a robust and organized knowledge base is an extremely useful tool to help close issues and help end-users utilize IT more effectively leading directly to increased service levels.

2.3 Service Operation

During the Run activities in the IT Operating Model, central IT will provide resources who manage the architecture and infrastructure to make sure the systems are performing at or above acceptable levels. These activities include:

- **Event Management**: In Event Management, central IT will be monitoring the environment based upon pre-defined thresholds to determine if an event occurs that requires action to resolve. Central IT will not only manage the performance of the environment but will look for trends and clues that help identify incidents and problems before they occur.
- **Incident Management**: Central IT will have standardized incident management processes with agreed upon handoff guidelines all tracking back to Service Level Agreements. IT support staff will make sure the end users are fully aware of the activities through the resolution process and follow-up at the end to make sure the incident is truly resolved.
- **Availability Management**: Not only will the central IT team focus on tracking events and resolving incidents and problems to minimize unplanned downtime, but as stated in the Change and Deployment Management area, central IT will work to make sure planned maintenance activities are kept to a minimum. Central IT resources understand that systems need to run on nights and weekends and even planned maintenance has a negative impact on the Departments.
- **Security Management**: The central IT architecture and infrastructure are maintained with Security Management as a guiding principle to allow resources who need access to systems to perform their jobs, but restrict others from information if they are not allowed to have access. The central IT team will monitor and maintain the security in the systems to validate that the security levels are correct as well as adding and removing access to systems to meet the requirements defined.
- **Service Continuity Management**: While central IT provides a resilient system design with redundancy at the core in case a disaster occurs, IT will also maintain up-to-date Business Continuity and Disaster Recovery (BC/DR) plans in place to make sure the State can quickly recover from any disruptions on service, no matter how large or small the impact to the systems.
- **Access Management**: Access Management is tied closely to Security management in running the operations for central IT. The IT team will be monitoring access to systems to make sure it is operating as designed. Also, maintaining access as resources change roles is a key function the central IT team will perform for proper Access Management.
- **Problem Management**: The central IT team will be tracking and monitoring incidents as they occur in the systems to identify trends that may lead to Problem Management. Central IT will then perform root cause analysis on the problem and work to close the gap in performance as quickly as possible.
- **Service Reporting**: Central IT will provide dashboards and detailed reports to IT stakeholders that are clear and succinct, with the right amount of detail to dive deeper into the reporting to help understand the health of the systems.
- **Request Fulfillment**: Central IT will handle service procurement requests through the consolidated State of Louisiana Service Desk. Service desk staff will answer questions about services and guide customers through the service procurement process.

- **Capacity Management**: Central IT is focused on maximizing the utilization of IT assets and will track and monitor the capacity of infrastructure on a continual basis. Using trend analysis central IT will predict when capacity will reach a maximum level and make recommendations for future procurement.

2.4 Technology and Infrastructure Management

Technology and Infrastructure Management provides a foundation for other services provided by central IT. The environment will be operated utilizing the following technology operations and applications management practices:

- **Technology Operations**: The purpose of the Technology Operations strategy is to help guide staff towards a common goal of providing excellent technology services. Technology Operations consist of operating system management, service desk, facilities operations, servers, network and equipment.
- **Applications Management**: The Applications Management process includes the support and maintenance of applications supported by central IT and delivered to customers through the published Service Catalog. Applications Management's goal is to deliver a consistent application service to end-users.

3.0 Service Portfolio Management

3.1 Service Catalog Management

The Service Catalog describes the Services that central IT provides to the various departments within the State of Louisiana.

The purpose of the Service Catalog is to provide information about available IT Services. The Service Catalog is used to support the delivery of IT Service to central IT customers.

The Service Catalog provides the following key benefits:

- A listing of the standardized set of Services that central IT provides to the customers of central IT with a brief description of the Services provided
- A communications vehicle for customers of central IT and central IT leadership to facilitate a common view of the work performed within central IT
- A starting point for discussions with central IT customers about the Services provided to either add, adjust, modify or eliminate Services if required

The Service Catalog is detailed in *Deliverable 10 – Service Catalog*. Updates to the Service Catalog are handled as part of the Customer Engagement process, as detailed in *Deliverable 14 – Customer Engagement Plan*.

3.2 Service Level Management

The Service Level Agreement (SLA) documents service measurements in place for the services central IT delivers to the departments within the State of Louisiana through the Service Catalog. The SLAs will be reported in regular intervals, as detailed in *Section 5.8 – Service Reporting*.

The purpose of an SLA is to provide a basis for measurements of the quality of the services between central IT and the departments who receive the services.

The SLA records a common understanding about services, priorities, and responsibilities for services provided by central IT. Each area of service has the level of service defined. The SLA specifies the levels of availability, serviceability, performance, operation, or other attributes of the service depending on the service description. The level of service is specified as the expected level of service which allows customers to be informed and what to expect at a minimum for the service assuming the service levels are achieved. The service levels are based on common business hours which are currently set from 9:00 am to 5:00 pm Monday through Friday, however the State of Louisiana Service Desk will soon be available 24x7.

Service Level Agreements are recorded in detail along with the corresponding Services in *Deliverable 10 – Service Catalog*. Updates to the SLAs are handled as part of the Customer Engagement process, as detailed in *Deliverable 14 – Customer Engagement Plan*.

4.0 Service Transition

The Service Transition process in the IT Operational Plan Framework includes the tracking, modifying, and testing of services delivered through the Service Catalog.

4.1 Change Management

The IT Operating Model framework (depicted in *Section 2.0 – Operational Plan Approach* section) provides the processes and tools required to deliver exceptional and proactive Operations support services, and the approach central IT will follow for Operations Change Management. Change Management is a process within the Service Transition function of the framework.

Central IT will provide and utilize an ITIL-based structured change management methodology to support the addition, movement, change, and/or deletion of all managed equipment and software. These changes will include all upgrades, patches, service patches and other mandatory or requested changes to the systems. Tracking will be done through a single ITSM suite which supports fully integrated, ITIL-based change and release management, includes a workflow engine enabling automation of change and release processes, and provides integration with the service management solution.

The Change Management process will be supported through detailed checklists and mandatory Operational Readiness reviews on large-scale changes and releases. This helps to make certain changes can be deployed successfully and that handoffs between all affected and participating teams have been completed. The policies and procedures used to manage change requests will be documented in an Operational Framework Document.

In Change Management, it is important that a common understanding is established up front among IT stakeholders regarding change policies and procedures to prevent the inappropriate use of Emergency or Urgent change procedures for poorly coordinated changes or changes scheduled too late to accommodate normal change guidelines. Central IT will provide the oversight required to validate changes are made in accordance with established Change Management process.

Central IT‟s Change Management process will align to the ITIL service management objectives where the goal is to minimize unintended impacts and prevent uncontrolled changes from jeopardizing system performance or service levels. Central IT will install the latest supported versions of software provided by the software manufacturers, at either N or N-1 version levels. As manufacturers release new versions, central IT will go through the Change Management process and test upgrades in non-production environments prior to installing such upgrades in the production environment.

Change Advisory Board (CAB): In accordance with ITIL best practices, the CAB reviews proposed changes to understand and assess the impact and service risk, and to authorize changes for implementation. The CAB also provides formal change approval/authorization through various media (i.e., formal meeting, electronic authorization, email and approval). They also:

- Review the status of each change throughout the change process

- Assess change priorities to develop a master schedule and an extended enterprise change calendar
- Verify implementation readiness and deployment checklist completion by all parties

When all steps are complete to the satisfaction of the CAB, the group approves the change for final deployment and implementation.

Central IT will define notification and routing requirements, approvers, and escalation requirements. Any change to a production service requires a Request for Change (RFC) to be recorded in the ITSM system. Low-risk and ongoing routine changes are typically staged as a recurring change and approved for deployment with only an infrequent review requirement such as annually.

Each change record provides a written description of each change and includes the following types of information:

- Change description
- Reason for change
- Planned start and finish dates and times
- Downtime requirements
- CIs impacted
- Testing to be performed and that which has been previously performed
- Implementation plan
- Cross-functional support requirements
- Post deployment verification steps
- Back-out/recovery plan

Change requests are routed to each stakeholder group for review using routing tables. Timing of these notifications and implementation requirements depend on the type of change. For example, IT implements emergency changes immediately to resolve production issues, whereas changes such as operating system upgrades are typically staged and scheduled months in advance. Central IT will use CAB meetings to review the pending Request For Change(s) (RFC)(s). Each meeting also recaps the previously completed requests. These meetings are also used to drive out planning schedules and review priorities to avoid conflicts.

Each RFC is required to be packaged and tested prior to deployment in an environment that will not impact production performance. Testing adequacy is verified by IT stakeholders according to the testing strategy described in the RFC. Changes are expected to be applied to test environments for verification prior to deployment into production. All failed/backed out changes and changes that cause production impacts are reviewed by the CAB as part of our Continual Service Improvement process. Changes that cause production impact are documented as an incident for tracking purposes. They may also be assigned to Problem Management for additional review, root cause analysis and follow-up. If the RFC was created to resolve an incident or problem, the associated Incident/Problem Record in the ITSM system is also closed.

The Change management process is fully integrated with incident management, problem, release, requests and configuration management, availability and capacity management. Change management is also integrated with project management, business continuity and continuous process improvement initiatives.

A high level view of central IT"s Change Management process is shown below.

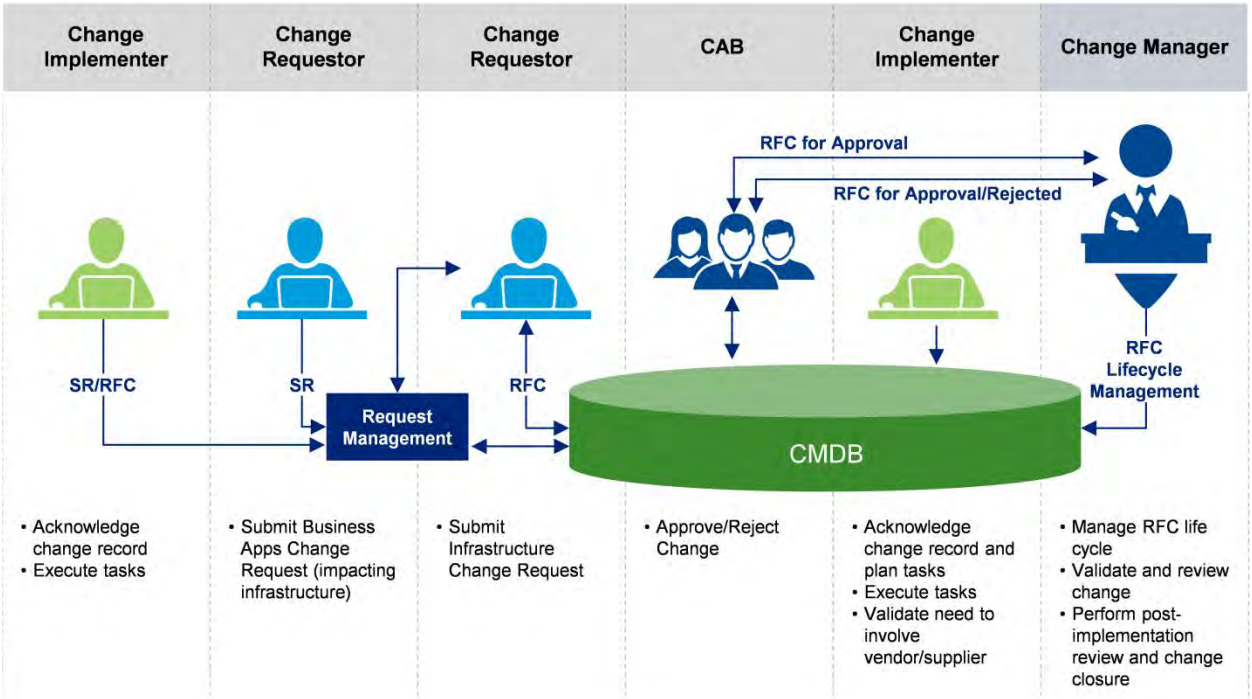

Figure 4.1.1. Change Management.

The high level roles and responsibilities within the Change Management process are:

- Change Requester
  - Initiate the request for change (RFC)
  - Confirm the RFC completion and provide input for the closure
  - Change Approver (Change Advisory Board - CAB)
  - Validate content
  - Confirm impact
  - Approve change request
- Change Manager
  - Validate format and information completeness
  - Coordinate assessment and change planning set-up (send draft tasks for schedule validation)
  - Assign tasks for build, test and implementation
  - Authorize change implementation

    - Perform post-implementation change review
    - Manage RFC cycle
- Change Implementer
    - Perform changes/tasks

4.2 Configuration and Asset Management

The purpose of Configuration and Asset Management is to establish and govern a robust inventory of IT assets, their configurations, and the relationships to provide trusted data to IT and enable improved efficiency, agility and reduced operational risk.

Central IT"s approach to Asset and Configuration Management, as integrated with overall operations management, not only empowers IT management to exercise dynamic control of IT items and assets, it also generates up-to-date data and verified status information on IT assets and infrastructure that are essential to other service management processes. The information on these components is stored in the Change Management Database (CMDB). The CMDB in turn contains all the data – the relevant Configuration Items (CIs) – which are required for the service delivery.

Asset and Configuration Management processes are central to many other ITIL operations processes that lead to efficient change management, including:

- Change and Release Management
    - Configuration Items (CIs) that are one version behind and in need of an upgrade are easily identified in the CMDB.
    - All Changes to Assets and CIs must be authorized and controlled via the Change Management process. Adherence to this policy is the critical factor in a successful service management organization.
    - Unauthorized changes can be detected by comparing what is in the CMDB with what is discovered in the environment.
    - The Definitive Software Library (DSL) includes all of the approved and tested images and software for each of the server types in the environment, enabling the quick deployment of a new server at the correct build level.
- Incident and Problem Management
    - As Incidents occur in the environment, they are associated with Configuration Items (CIs). A description of the CI exists within the CMDB, including information about what applications the CI supports, the impact of an outage to the CI, and associated Service Levels of the CI. This enables the support team to quickly understand the CI, what is affected by it, and helps understand how to better support the environment
    - As incidents reoccur in the environment, by the fact that the incidents are linked to CIs, trending can detect if a specific CI is having recurring incidents and should enter the Problem Management process to understand the root cause of the problem, and potentially leading to the replacement of an intermittently faulty system

Central IT should select one ITSM tool with the following Configuration Management features:

- Provides a CMDB as a single source reference for IT
- Automatically discovers IT assets, applications, and relationships
- Presents a dashboard with interactive access to key metrics
- Integrates with the other components of our solution for Incident, Problem, Change, Release, Capacity, and Availability Management as well as Service Level Management and Financial Planning

Moreover, the Asset and Configuration Management solution includes the types of assets, CIs, and components along with their attributes, logical and physical relationships. Configuration items and asset items are separate entities in the CMDB. While all assets are classified as CIs, logical IT elements (non-assets) that are viewed as part of the CMDB infrastructure used to deliver the services are also classified as CIs.

The figure below depicts the ITIL-based Asset and Configuration Management process and role assignments.

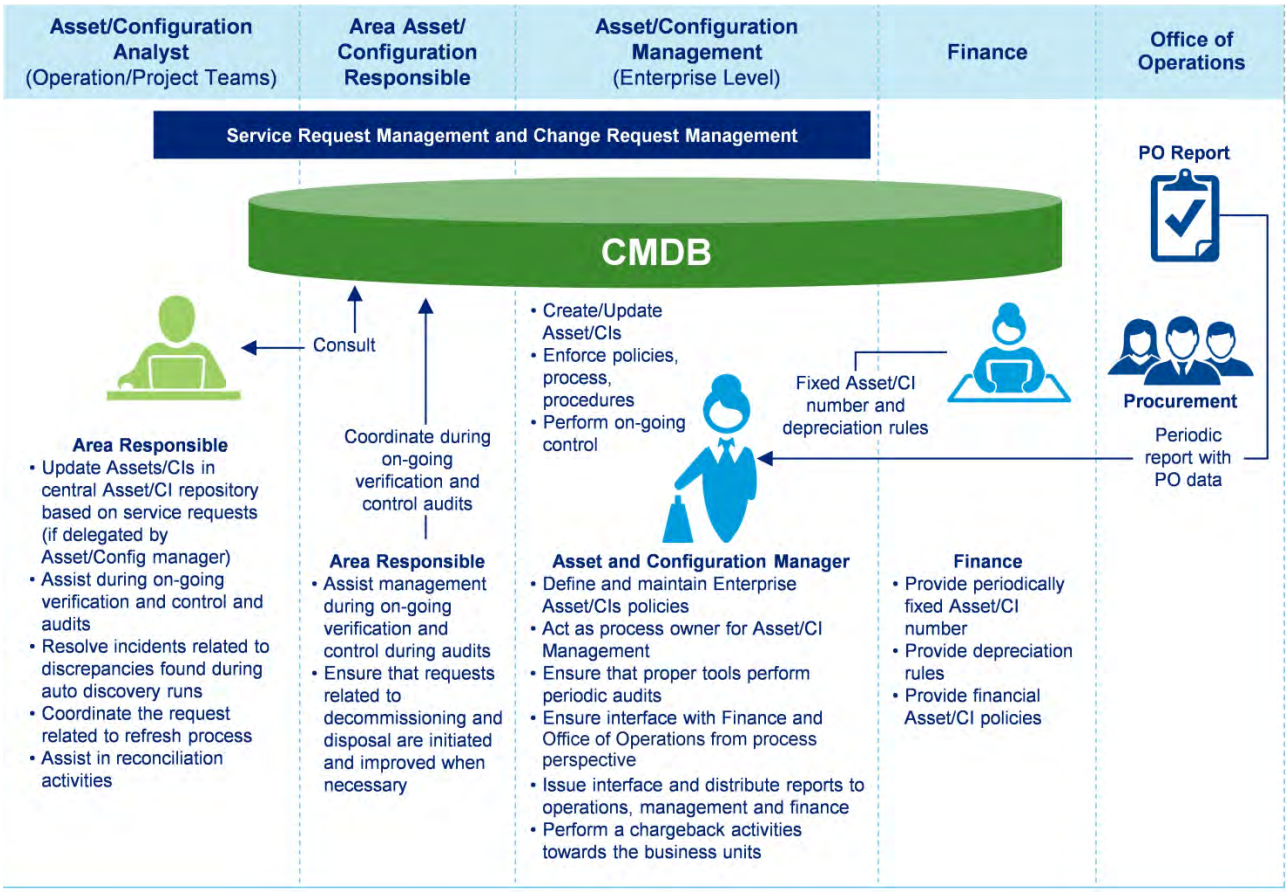

Figure 4.2.1. Asset and Configuration Management.

Within this diagram, the configuration analyst and the configuration management activities that take place to maintain the accuracy of the Configuration Items (CI) are shown.

- The Configuration Items are maintained in the CMDB. CIs are verified against change records
- Policies and procedures of the process are the responsibility of the Asset Manager
- Financial information about configuration items are the concern of the asset management process and are passed over to finance

Consistent with the ITIL based approach, the Asset and Configuration Management process manages the full life-cycle of the IT assets and CIs and establishes audit requirements and rules. It provides guidance on audit requirements and compliance through on-going training.

4.2.1 Configuration Management System

The Asset and Configuration Management approach and processes will be supported by the single ITSM tool. The implementation of the ITSM tool incorporates information from multiple databases that contain details of the components or CIs that are used in the provision, support and management of IT services. It will provide a “single source of truth” for the State of Louisiana‟s IT infrastructure, including IT operations and service support. As such, it will provide a complete, accurate, and up-to-date view of the people, processes, and technologies that make up the Departments‟ and IT environment.

The ITSM tool will manage physical information and provide process control over IT services and infrastructure service components. It also will record and manage contractual and physical information on all newly purchased and existing IT assets and provides incident management data to associate with configuration data. It will also incorporate the information that relates to the maintenance, movement, and problems experienced with the CIs.

Central IT will use the configuration management reporting function of the tool to provide monthly reports on configurations and CMDB data currency. This includes:

- CI and CMDB exceptions
- Numbers and classifications of changes to CIs
- Trend analysis of the changes made

The Asset and Configuration Management tools and processes will provide accuracy, validity, integrity and control of the CI (Configuration Item) data, while facilitating all IT service delivery processes. Configuration Management controls the entire CMDB, the core of all IT delivery services. The solution also:

- Provides Configuration Management planning and CMDB structure definition in conjunction with the agencies
- Creates/updates CI records and assets defined as within scope
- Supervises asset data verifications, physical inventories and audits for agencies approval
- Controls the creation and maintenance of asset classification and categorization in the CMDB
- Verifies Configuration Management data

4.2.2 Configuration Management Governance

Configuration Management governance will create a recurring Configuration Management meeting charged with reviewing and approving all changes to the State of Louisiana"s configuration management, tools, and processes which are implemented through the ITSM tool. The recurring Configuration Management meeting"s primary purpose is to verify that all State configuration items are changed in a controlled way and that the Configuration Management Team adheres to and enforces the Configuration Management processes. The recurring Configuration Management meeting also provides a venue for reviewing trending and assessing current process efficiencies and continuous improvement opportunities.

4.3 Service Testing, Release, and Deployment Management

Service Testing
Service Testing, Change and Release Management processes are used to deploy upgraded software and patches. Central IT assigns a release manager to lead a release and testing coordination team. The Release Management process requires that software releases be packaged and tested prior to deployment. Testing adequacy is verified according to the testing strategy described in the change record. Changes are applied to test environments for verification prior to deployment to production. Software is certified once it is tested and meets the certification criteria. All failed and backed out changes and changes that cause production impacts are reviewed by the Change Advisory Board (CAB) as part of the Change Management process. Changes that cause production impact are documented as an incident for tracking purposes.

For each software upgrade, central IT will evaluate the upgrade, and test its impact for functionality, stability, and performance before submitting for review and acceptance to the agencies. Central IT will work to resolve any issues identified during testing. In the event that an issue cannot be resolved, central IT advises the agencies on the impacts of proceeding with the upgrade, or of not performing the upgrade. Central IT follows an industry-standard patch management process. The following activities are included in the overall patch management process.

Assessment activities include:

- Patch administrators continuously monitor infrastructure components, vulnerability, and patches, and evaluate vendor-reported levels of criticality
- Verifying that all information regarding new patches is documented and communicated across service delivery and client delivery teams
- Verifying that the recommended patches are applicable for each environment

Impact evaluation activities include:

- When new patch alerts are requested, the central IT team will download and review the new patch
- The central IT team will categorize the criticality of the patch according to the following:

  - **Emergency**: An imminent threat to the State"s environment. This is considered a RED ALERT and the Central IT will follow the process to implement the required patch immediately
  - **Critical**: Targets security vulnerability. Impact to environment will be assessed and the patches will be scheduled for deployment ASAP
  - **Not Critical**: Standard patch release updates. Follow standard patch schedules
- Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing, and verifying. The operational impacts of implementing a patch will be assessed

Testing activities include:

- Implementing patches on test systems and testing for any operational or functional changes caused by installing the patch
- Maintaining testing results for audit and verification purposes

Certification activities include:

- Comparing testing results to certification criteria
- Preparing the patch for deployment

Deployment activities include:

- Implementing security patches in accordance with stated critical timescale, (critical, high, medium, low)
- Patch administrators develop a comprehensive documented rollback plan for all patch deployment
- Patch administrators follow the Change Management process
- Patch administrators determine that the patch deployment request is approved by the departments or that a wavier form has been completed

Post implementation activities include:

- Verification is performed to verify that patch implementation was successful

Central IT will certify software upgrades and security patches for any third-party software to support the systems before releasing them for installation to UAT, training, and production environments.

Software Deployment
Central IT will deploy software using best practices and procedures to follow the most appropriate method in terms of controlling versioning, licensing and managing change through software distribution, and monitoring the system configurations to provide stability and consistency. The majority of software updates and patches, including operating systems and anti-virus software, are deployed using the server

automation tool. For other third-party software, central IT manually creates the system images for the servers, following the prescribed installation and configuration instructions. Once the image is tested and certified it can be replicated to other systems automatically.

Software Updates
Central IT will download and apply service packs and security patches for third-party Software components for the State of Louisiana"s environments (UAT, Training, and Production) and devices regularly recommended by third-party software vendors through the Term of the Agreement. Service packs and security patches updates shall be downloaded to a central repository tested and certified by central IT before deployment to the UAT, training, and production environments.

Central IT will update security and anti-virus software components for the State"s environments and devices regularly through the Term of the Agreement, with the latest software, patches and anti-virus definitions available from the manufacturer. Security and antivirus updates will be downloaded to the central repository. These updates are tested and certified by central IT before deployment into the UAT, training, and production environments unless a department request that the updates be tested separately by the department prior to the update moving into production.

Central IT (along with its solution software vendors) will analyze monitoring reports to search for anomalies on a periodic basis: weekly, monthly and quarterly.

Software Reporting
Central IT will provide the software component report for the managed software assets so the departments can have confidence in the accuracy and reliability of the information.

Central IT maintains software components as CIs within the CMDB. Reports will include:

- Current inventory, by server, of all software components with version numbers in use and latest version number available from the manufacturer
- Software upgrade status, upgrades in progress, planned and accepted for exception
- Number of licenses procured and in use for each software component
- Owner of each software component
- Support level and expiration date of maintenance agreements for each software component
- Any major upgrades announced by manufacturer of a software component to be released in the next year

Central IT provides software reporting as a component of Asset Management in which each software component is a CI within the CMDB. The CMDB links the relationship of CIs together to provide meaningful reporting, for a wide range of IT service management processes. The CMDB allows Central IT to quickly respond to the departments" requests for an updated list of open source software annually or per request.

4.4 Knowledge Management

Knowledge management is the transfer of knowledge from one entity to another, which enables the recipient to benefit from already-posted issue identification and problem resolution. The goal of knowledge management is to improve the quality of decision-making by defining that reliable and safe information is available during the service lifecycle. The knowledge management processes confirm the capture of knowledge across the service management lifecycle into a service knowledge management system which is made available to all information stakeholders.

Central IT"s knowledge management solution provides access to a searchable library of FAQs, articles, known errors, how-to documents, resolutions, and announcements. Knowledge articles can be created from incidents, problems and error records. Knowledge articles can also be imported from external sources including HTML files from third-party help desk applications. The figure below illustrates the variety of search options and sources available.

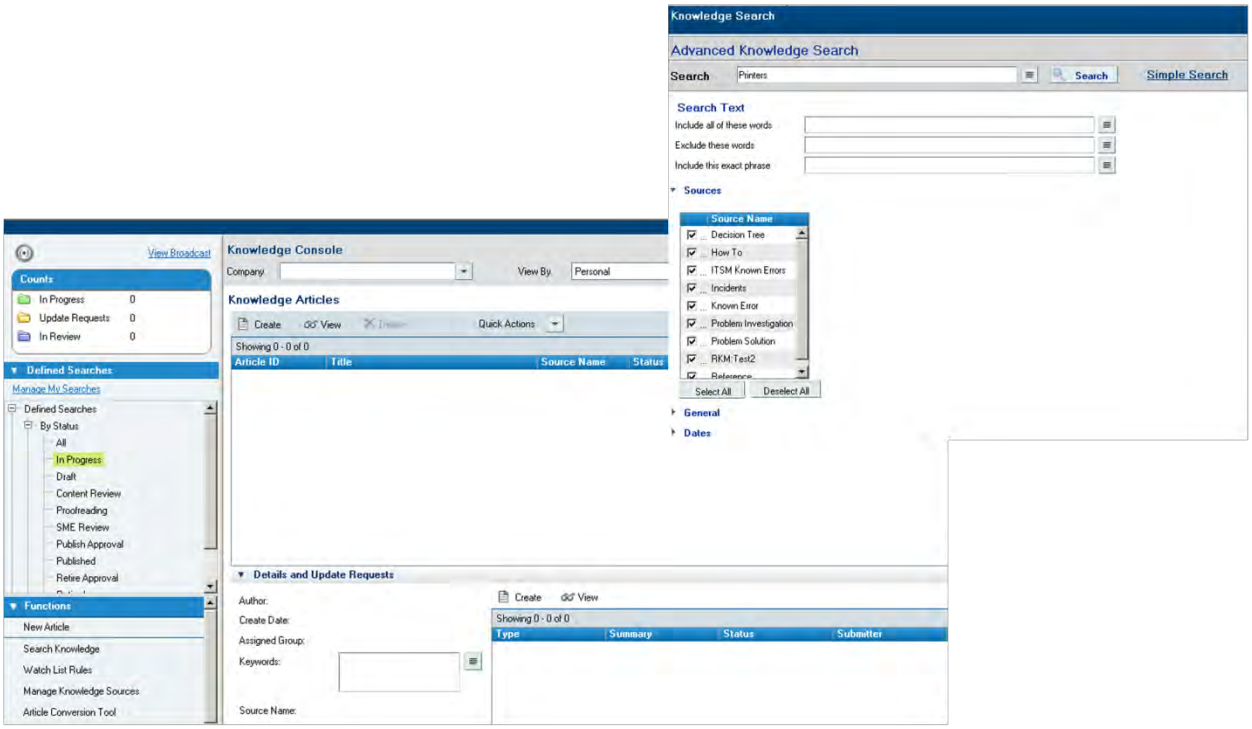

Figure 4.4.1. SR Knowledge Management Console.

Service Desk staff can search the knowledge base for answers to questions related to the functionality of the system to quickly assist a user, resulting in an enhanced customer experience. For example, if a department staff member is experiencing an application problem in Statewide Email requiring a temporary workaround while the application is fixed, the knowledge management system is updated with the workaround information. When staff from another department experiences the same issue, the Service Desk staff checks the knowledge base and is able to take advantage of the workaround. Productivity and efficiency are perpetuated through this approach.

A version of the knowledge base will also be provided to State of Louisiana staff to provide them with knowledge articles and FAQ"s for self-help. The knowledge articles can also provide end-users with tips on how to use technology more effectively to better utilize IT resources.

5.0 Service Operation

5.1 Event Management

Event Management includes the gathering, analysis and presentation of information from network and security devices, identity and access management applications, vulnerability management and policy compliance tools, operating system, database and application logs, and external threat data. The Event Management solution provides log auditing and review and supports cyber incident response.

As part of the Event Management process, there are five sub-processes employed by central IT for effective event management:

- Event Detection
- Event Filtering
- Event Prioritization
- Response
- Event Close

Event Detection
Central IT will maintain an enterprise monitoring solution to collect, filter, and report key metrics and system events for all supported equipment and systems. Metrics and system events are collected either through SNMP notifications or a dedicated monitoring agent that reports to the enterprise monitoring solution.

Central IT implements log collectors on UNIX operating systems. Devices which do not support standard syslog messaging, such as Microsoft Windows, require the use of a log agent. Central IT will maintain a list of metrics and events to collect from monitored devices and systems. Errors in the reporting process will follow the Incident Management process for resolution.

Event Filtering
Before being sent to the central monitoring tool, the collection agent will determine which metrics and events should be sent. Event filtering policies determine these actions, and are set proactively by the central IT monitoring team to capture the critical metrics and abnormal events. Even when not recorded by the central monitoring tool, the local monitoring agent will record the metrics to its log files for debugging purposes.

Event Prioritization
Once the central monitoring tool has collected the metrics and events from the monitored systems, the tool will determine the priority to be given to the event.

- **Informational:** The event does not require follow-up action, and is recorded for informational purposes only. The events and/or metrics are recorded in the log files and maintained in the monitoring tool database. Informational events are useful to determine KPIs, such as CPU spikes in a given time.
- **Warning:** The event is approaching a predetermined threshold. Thresholds are determined by central IT to determine when metrics such as CPU usage, disk space capacity, and other

indicators reach near-critical levels. Notifications for warning events are sent to the appropriate IT administrators to resolve the issue before a service disruption occurs.

- **Exception:** The event has impacted service quality or availability, and needs to be resolved immediately. For example, a server may have been rebooted or a network device may have gone offline. Business users are facing service disruption, so notifications for exceptions are sent to central IT leadership, as well as IT administrators to resolve the issue.

Response
Once the event has been prioritized, notifications will be distributed using notification policies established in the central monitoring tool by central IT. The notification policies determine which IT stakeholders and teams are notified for each type of event at each priority level. Notifications can be customized to be sent by SMS text notifications, email, or phone.

In addition, the central monitoring tool is integrated with the State of Louisiana Service Desk solution to automatically log an appropriate level service request for events deemed warnings and exceptions. The Service Desk solution will automatically assign a central IT team to resolve the issue and close the ticket.

Should the ticket not receive a confirmation response within the published SLAs, the ticket will be escalated automatically, as described in *Section 5.2 – Incident Management.*

Close
Once the issue has been resolved, the central IT team will close the ticket within the State of Louisiana Service Desk solution as detailed in *Section 5.2 – Incident Management*. This process will automatically close the alert notification within the central monitoring tool.

5.2 Incident Management

Initiation
When an incident, request or problem is received by the service desk, the analyst opens a ticket in the Service Desk tool documenting the required information and identifying the severity of the issue. If the issue cannot be resolved by the Level 1 service desk, the ticket is assigned to a Level 2 or Level 3 support group. The support group then attempts to resolve the issue by first referring to historical information by looking it up in the system knowledge base, as detailed in *Section 4.4 – Knowledge Management*. If the issue has not been encountered before, the team will use traditional problem-solving techniques (e.g., recreation of the problem, reviewing system changes that could have unknowingly caused an issue, known software issues, etc.) in an attempt to come to a resolution.

Resolution
The service desk will keep the originator of the ticket informed of the status of the request as it goes through the resolution process. A status update is provided on an interval appropriate to the priority of the incident. The assigned service desk analyst confirms incident resolution with the originator prior to closing the ticket. Once the issue has been resolved, the service desk analyst records information such as the end date and time when the issue was resolved, the actual cause of the incident, the action taken to resolve the incident, as well as any future action that may be required. After the ticket has been closed, the knowledge base is updated with the issue, resolution, and the steps taken to reach the resolution. A customer satisfaction survey is generated to the originator of the ticket upon closure of the ticket. The

customer satisfaction survey tool alerts the service desk manager if a survey response is below the expected level. Each poor survey response is treated as a complaint and is attended to by the Service Desk management team.

Escalation

Central IT recognizes that issue escalation and consistent communications is important, and understands that production environment problems can have severe business impacts. The escalation process is a built-in feature to the Service Desk solution. Once a request arrives, the escalation process handles the escalation appropriately based on severity. Each severity level has a "trigger" that determines when it is appropriate to institute the escalation process. The foundation of this process is that communications of a situation where a target response time is in danger of being missed is appropriately disseminated among the key stakeholders of both central IT and the affected agencies. The Service Desk ticketing system Service Level Management module is configured to alert the service desk and the group responsible for resolving the issue. The escalation matrix maintained by central IT will be used to set the expectations. Central IT maintains the contact list for use with the escalation procedures and confirms the service desk has access.

This list contains three-level deep contact details for key personnel including:

- State of Louisiana Service Desk
- Vendors
- Technical specialists required for operational troubleshooting

Major Incident Management

Central IT uses a standard ITIL-based process for managing major incidents which require significantly higher visibility and much more stringent procedural requirements. Major incidents are managed by a central IT SWAT team which is led by a central IT SWAT manager.

The SWAT manager creates the specialized processes to address the major incident and identifies any facilities required such as establishing emergency conference bridges, "war-rooms" and the communication methods to be used (e.g., email, instant messaging, cell phone, and collaborative work spaces).

The SWAT manager also identifies a pre-determined list of technical support personnel and management escalation contacts from within central IT, affected departments, and any necessary third party support groups.

Call lists and escalation requirements are documented per central IT policies and procedures. Each support team resource is trained on the processes documented therein. These trained resources are called upon in the event of a major incident.

The SWAT Team is dynamically invoked in situations such as a major application component failure, security incident, or other extended service outage. SWAT Team members perform their other assigned responsibilities on a daily basis. Each is also on-call and available to join the cross-functional Recovery Team when called on by the incident manager. The incident manager provides management oversight and coordination of each major incident from identification through resolution, including:

- Initiates the declaration of a major incident and engages the SWAT Team
- Coordinates analysis, tracking and recovery efforts and provides communications between the designated Recovery Teams until incident resolution
- Keeps the project team and affected departments informed of changes in incident status throughout the incident life-cycle, in accordance with project policies and SLAs
- Keeps central IT management informed of anticipated resolution times for active major incidents

Following the resolution of each major incident, a problem record is automatically created and the incident manager conducts a post-mortem review with recovery participants.

This typically includes stakeholders from central IT, the affected departments, and appropriate third parties. The goal is to analyze root cause(s) and identify action items and areas for improvement to prevent the problem from recurring. The team also looks for areas that can reduce recovery times and improve team performance on future events as part of the continual improvement process.

5.3 Availability Management

High system availability is a primary goal of IT solution design. All of the components of central IT"s solutions will be designed to provide an integrated system that meets and exceeds the availability requirements identified by service and IT stakeholders. In short, the design goal is to have the State"s systems available to meet needs of application users when and how they are needed.

This section discusses central IT"s solution design features to be implemented so the State"s systems environment is a robust, highly available solution and meets these timelines.

Central IT follows an Availability management process that identifies the availability requirements, the potential causes of outages, and the infrastructure and application redundancy and safeguards that are required to consistently achieve the required availability. Central IT"s comprehensive approach to achieve and exceed the availability requirements consists of a two pronged approach:

- Operational processes based on our Systems Operational Framework (SOF) that provide stability and minimize human error
- A robust Technology Architecture that is designed with high availability in mind

Availability management cuts across many of the processes within the IT Operational Plan Framework. The availability management process approach can be broken down into the following views:

- **Establish availability requirements:** Central IT will analyze the current SLA"s, identify what is working well as well as areas for improvement, and establish an acceptable baseline based on the analysis.
- **Design for high availability:** System design includes redundancy and failover at all levels, creating no single point of failure.
- **Elimination of human error:** Adhere to established policies and procedures, driving high availability and stability in the environment. This includes:
    - Creating, maintaining, and providing clear operational documentation

  - Increased use of automation
  - Restricting privileged systems access to only those users that require it
  - Strict adherence to documented policies and procedures
  - Utilize effective monitoring–enabling the rapid response to an outage event when it occurs, and also enabling proactive measures to be taken in the event that thresholds (such as capacity utilization) that can impact availability are being approached
- **Preventative Maintenance:** To make sure that central IT has applied available fixes to known problems and security exposures
- **Rapid resolution:** To quickly resolve outages when they are detected, through automation when possible, through failover if needed, or through the use of diagnostic tools and resolution processes by our skilled technicians

Additional detail on key IT Operational Plan processes and procedures that enable central IT to achieve high availability for the State of Louisiana"s systems include:

Preventative Maintenance: Preventive maintenance is performed to avoid application glitches and component failures. Central IT will work closely with agencies and third-party vendors to recover affected component expediently. Furthermore, central IT follows the latest industry standards when it comes to proactive IT maintenance. Examples include the routine backup of databases, operating system images, or the code repository; the application of non-system critical patches that do not require a system reboot; disk management; SAN storage allocation; VM resource management (e.g., CPU, memory), etc. For routine maintenance such as a non-critical bug fix or feature update, central IT will perform these only within the scheduled downtime maintenance windows.

Hardware Maintenance: Central IT"s hardware maintenance plan includes:

- Deliver the correct and timely support for hardware assets
- Leverage single-call/single-ticket accountability in providing multiple vendor hardware/software support
- Minimize downtime and protect against outages
- Accelerate recovery by working directly with the hardware and software vendors

Central IT follows industry standard schedules for routine hardware maintenance. All State hardware will be configured to be closely monitored. Any failed or underperforming hardware will be replaced immediately, consistent with the stated SLAs, to minimize the impact on performance and functional requirements.

Third-party Software Maintenance: Central IT follows industry-standard schedules for routine software maintenance. State software will be configured to be monitored closely. Any failures or degraded performance will be immediately reported to the appropriate vendor.

Central IT will also implement all security and critical updates recommended by third-party software vendors on an as-needed basis to help prevent future issues.

Handling Component Failures: When component failure is a result of hardware failure or underperforming hardware, central IT will coordinate with the respective hardware vendor for a quick resolution and/or replacement of the affected hardware component.

New hardware for critical systems will be redundant within either one of the primary data centers or spread across multiple primary data centers. Therefore, critical systems with the redundant configuration will not experience long-term outages in the event of any hardware failures. The solution is developed to leverage as much automated failover to redundant hardware as possible. In situations when the failover to redundant hardware is not automatic, operations personnel will follow manual failover processes guided by leading practices that provide for rapid remediation.

Accordingly, the respective hardware vendor will determine if the hardware can be repaired or it must be replaced. The affected system component will remain out of service until authorized personnel approve bringing the system back into service. Repaired or replaced hardware can be optionally brought up as a redundant hardware component. If it is deemed necessary to bring the replaced hardware back into active mode, it will be brought back to service in an after-hours maintenance window.

Backup and Recovery: Good system design always considers the worst case scenario and provides appropriate coverage. Central IT systems are designed to support backups within the primary data centers (for fast retrieval) as well as backups to tape in case of a disaster that makes the data or systems at the primary data center(s) inaccessible. The recovery of data that is backed-up can be used in other scenarios as well. The backup and recovery solution lets administrators restore lost data if necessary. Recovery can also be made to return to a cleaner, older version of the data or an entire operating system configuration.

Change Management. The implementation of and adherence to a disciplined Change Management process is key to providing stability in the environment. Central IT‟s solution for Change Management, as described in *Section 4.1 – Change Management*, provides that stability.

Central IT‟s Change Management process provides:

- Strict controls around the environment to prevent unauthorized changes
- Documentation of the details of the change, including what will be done, what systems and applications will be affected, what the risks are, and what the back-out plan is
- A detailed back-out plan, in the event the change is not successful
- Thorough testing of all changes in a non-production environment, before moving to production

By following the IT Operational Plan framework procedures such as those listed above, central IT is able to create an environment that is stable and predictable, by controlling change, minimizing human error, maintaining hardware and software at current supported levels, and quickly escalating and resolving issues when they do happen.

5.3.1 Availability through Technical Architecture

As complex systems inherently have more potential failure points and are more difficult to implement correctly, central IT understands that adding components to system design can undermine the effort to achieve high availability. Central IT‟s technical architecture approach, as detailed in *Deliverable 08 – IT*

Technical Architecture Model, has a straight-forward but robust design that minimizes the impacts of single outages and eases maintenance activities such as patching and upgrades.

Central IT will achieve this advanced robust design by incorporating five key architectural approaches:

- Load balancing
- Redundancy
- Failover
- Virtualization
- Error detection and correction

The first four items in the list above (load balancing, redundancy, failover, and virtualization) combine together across all technical aspects of the technology architecture to create a solution with no single point of failure.

The fifth item in the list above (error detection and correction) encompasses the technology and tools used to identify issues when they occur (and if possible before they occur) and to quickly correct them.

Additional detail of each is provided below.

Load Balancing
A robust load balancing implementation contributes to the reduction of bottlenecks that impact system availability. Load balancing is a methodology to distribute workload across multiple servers, network links, central processing units, disk drives, and other resources to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload.

Redundancy
Redundancy is the duplication of system components or functions with the intention of increasing reliability by reducing single points of failure through the implementation of backup or fail-safe components. To maximize the benefit of component redundancy, central IT"s technical architecture plan includes the following:

- There are redundant data centers
- All power supplies for all hardware components are redundant
- All servers have redundant network interfaces
- Storage is SAN-based whenever possible with built-in redundancy at all levels, including:
    - All hard disks are configured in a redundant array of independent disks (RAID) configuration
    - All hard disks have hot spares
    - The SAN contains redundant controllers
- Network connectivity switches and routers are redundantly configured in case of a hardware, network cable or network card failure
- Each location includes a redundant network circuit
- Servers (web, application, database, etc.) are implemented as an active-standby pair or as an active-active server farm

Redundancy is implemented using both passive redundancy and active redundancy concepts. Passive redundancy reduces the impact of component failures by using excess capacity as hot spares. Active redundancy eliminates performance decline by monitoring performance of individual devices and reporting before a system or functionality becomes unavailable.

Failover

If a system component does fail, central IT"s solution includes redundant systems (as described above) that will automatically failover. For instance:

- Systems spread across multiple data centers, such as Statewide Email and the network core, can recover in the alternate primary data center in the event that there are one or more issues affecting system availability, performance, or data integrity.
- Virtualization clusters provide for automatic failover; switching a failed system to a redundant or standby system.
- Network load balancers are used to switch to a redundant or standby system upon the failure or abnormal termination of a previously active application, server, system, or network device. This means that in case of a system failure, failover can proceed without requiring human intervention.

As discussed above, hardware deployed will include redundant components for the storage disks and network interfaces. In the event of a hardware problem, the systems will be able to failover to the redundant components.

Once the problem is detected, fixed and the affected system component is determined ready to be brought back into production, failback will be performed. Failback is the process of restoring a system, component, or service that is in a state of failover back to the state it was originally in before failure.

Virtualization

The use of virtualization software allows failover practices to become less reliant on physical hardware. Central IT"s solution provides a virtual machine (VM) platform to provide seamless server scalability, redundancy and availability.

The solution maximizes hardware utilization by allowing authorized personnel to perform planned hardware maintenance without interrupting service or compromising cluster availability. The solution continuously monitors utilization across a resource pool and intelligently allocates available resources among VM"s based on application needs.

In case of a hardware failure, the virtualization platform allows server administrators to migrate the affected VMs from one server to another while the VMs continue to run with no impact to end users. Another feature of the solution is the ability to proactively move VM"s away from underperforming servers and to migrate their disk files from one data store to another without disrupting end user service. The solution also allows server maintenance and patch application to be performed without scheduling downtime or disrupting business operations.

Error Detection and Correction

Error detection is another key element of central IT"s solution that is crucial to high availability. Error detection identifies the affected component, so that support teams and users are notified, and errors can

be corrected as quickly as possible. Error detection helps administrators detect potential issues before they become problems.

Central IT"s monitoring solution will include the capability to monitor each of the types of servers, network devices, databases, batch jobs (including backups), and application services to determine if they are functioning as designed. In the event there is an issue, the monitoring tools will generate an alert that will automatically create a ticket in the ITSM system so that work to correct the issue can begin immediately.

To meet the availability requirements for the State of Louisiana"s systems, central IT will:

- Implement a technical architecture with no single point of failure, as defined in *Deliverable 08 - Technical Architecture Model*
- Schedule all changes and maintenance activities outside of the stated hours of availability where possible, and following the documented change approval process
- Schedule all batch jobs (including backups) outside of the stated hours of availability where possible
- Provide staffing to State of Louisiana Service Desk and Support teams 24x7x365 to be able to quickly respond to unplanned outages should they occur
- Define a process to extend/adjust the hours of availability as needed by the agencies and as approved by the central IT leadership

5.4 Service Continuity Management

Service Continuity consists of availability management, business continuity, and disaster recovery. Availability management is detailed in *Section 5.3 – Availability Management.* Central IT"s systems business continuity (BC) and disaster recovery (DR) approach minimizes the possibility that major catastrophic events will disrupt the State of Louisiana"s systems.

Central IT"s approach to BC and DR for the State of Louisiana"s IT systems has three components.

- Central IT"s system architecture incorporates mirrored system architectures at the primary data centers ISB and DPS for critical systems.
- Central IT has a consolidated disaster recovery contract for critical data and systems to be recovered outside the Baton Rouge geographical area.
- Central IT will meet State policies and procedures to meet desired uptime requirements, availability and capacity management standards, and applicable SLA provisions.

The framework provides an effective set of processes and controls for integrating all aspects of the operation of complex information technology systems, from daily routines to exception conditions such as natural disasters. The business continuity and disaster recovery processes are part of the Service Continuity Management within the framework.

Central IT conducts a four step process initiated during the transition that is summarized in the figure below.

Figure 5.5.1. Process Developing Process and Procedures.

Central IT"s analysis, planning and implementation steps include:

- **Conduct a High Level Business Impact Analysis (BIA):** System requirements, functions, and interdependencies are reviewed by central IT and agency stakeholders. The results are used to identify system contingencies and set priorities for recovery based on operational impact.
- **Confirm the RTO:** Critical to DR is validating the recovery time objective (RTO). The RTO is the overall length of time an IT component can be in recovery before it negatively impacts critical business processes.
- **Architect Recovery Process and Procedures:** In developing each DR procedure, central IT will address network requirements, infrastructure needs, software recovery, application recovery, data recovery, record management, and security and compliance.
- **Testing/Training:** Central IT employs various levels of BC/DR testing, with varying degrees of agency involvement.

Aligning plans and the real life needs of the agencies is also encouraged by central IT"s approach. Central IT conducts structured walkthroughs with key technical resources, verbally assessing the plan. Simulation testing will also be employed in which a disaster is replicated so the process can be implemented with full interruption testing, in which case the DR plan is activated in total.

5.4.1 Business Continuity/Disaster Recovery

Central IT"s primary data centers ISB and DPS are located in close proximity in the Baton Rouge area. To minimize the impact of a large-scale disaster, central IT will procure a consolidated DR contract with a third party to host DR systems in a geographically diverse location. The Facilities strategy for the future-state design is detailed in *Deliverable 16 – Facilities Management.*

For critical systems such as ERP and Statewide Email, the architectures will be designed to failover from one primary data center to the other. System data will be replicated either in real-time or nightly depending on the criticality of the system. This high-availability strategy will be employed for any disaster local to the affected data center. The strategy provides the following (which are described in more detail further below):

- Daily backups of the critical systems, created by the CommVault tool via SAN
- Processes and procedures to mirror the configuration of the systems
- Sufficient capacity to meets the systems performance requirements
- Network and systems configurations (maintained through Configuration Management and replicating the changes from Production to the secondary site) to enable the interfaces with external systems

The solution is designed to provide for continuous near-time replication of the databases and nightly replication of non-database data. Accordingly, if a disaster strikes the primary data center for a critical

system (such as Statewide email at ISB), the system stands ready to be cutover to the secondary facility. In such instances the DR systems would promote the secondary facility to production and activity would be cutover to the secondary facility systems.

Best practice calls for the cutover decision to be made by management, however, once the decision is made automated processes will orchestrate the actual cutover. This capability will enable the restoration of production system functionality within the published SLAs.

The non-database software and configurations will be replicated to the alternate data center using an industry-leading backup and restoration tool. Accordingly, every change to configuration of software, hardware, networks, ports and interfaces is replicated at the alternate site. The alternate site will have the current version of the code and the last major release version of code.

Automated failover to the alternate site will be application-specific and will be facilitated by a workflow automation tool that can be configured to take actions upon the occurrence of specified

In the event a restore is needed from an old backup (due to some data corruption for example), the data is restored from the copy at the alternate site (which is backed up with the rest of the systems there). This eliminates the cost of labor for management and tape storage, while providing enhanced capabilities.

For all systems that require restoration in the event of disaster, central IT will procure and maintain a consolidated disaster recovery contract with a third-party vendor. The contract will enable disaster recovery at a site outside the Baton Rouge geographical region. This will allow systems to be restored even in the event of a large scale disaster affecting the metropolitan region. All customer departments" critical systems will be added to the DR contract after review by central IT and department IT stakeholders.

To verify the DR Plan and preparedness, an annual assessment will be performed to demonstrate integration and alignment of plans across the State"s systems. To keep abreast of new business requirements and evolving threats, central IT will perform tests in support of the BC/DR plan, and will report the results to the department leads. These tests will include:

- Procedures and activities to support the restoration of critical applications and infrastructure
- Procedures and activities to support Capitol Park users and connections
- Procedures and activities to support remote users and connections

5.4.2 Disaster Recovery Restoration

In the event of a minor or moderate event, central IT will restore the supported systems in the timeframes defined in the published SLAs. The requirements and levels for service recovery following a disaster or disruption are different for each area and are described in the SLAs. In the case of a major event affecting both primary data centers in the Baton Rouge area, however, the systems will have to be restored utilizing the DR contract with the procured third party provider.

This all-encompassing DR capability addresses the areas of infrastructure, software, and data, including tapes, external hard drives, primary databases, email and all other major enterprise components.

Adherence to this approach will provide seamless transparent recovery of the supported State of Louisiana environment.

5.4.3 Disaster Recovery Reporting

In the event that both primary data centers are impacted by a major disaster, central IT will provide an initial assessment of the damage and will provide initial restoration/replacement plans. This report will be submitted to the departments and central IT leadership for review and acceptance. Central IT will also provide to the agencies a comprehensive assessment that includes a restoration and replacement plan for the primary data centers.

Additionally, a Contingency Management Report will be generated every time the DR plan is tested or used. The report shows the number of times the DR plan was used or tested and the effectiveness of its use. When the plan is activated, a description of the incident that initiated the situation is reported in case changes need to be made. The report will assist management in determining:

- Whether the plan is accurately maintained and tested on a regular basis
- Whether risk analysis has been carried out as required
- Whether the plan has been updated in accordance with changes
- Whether lessons learned from any actual use of the plan have been incorporated
- Whether the costs of testing or using the plan are in line with forecasted costs
- Whether SLAs are being met through the use of the plan
- If change requests are needed to improve or enhance the overall effectiveness of the DR plan

5.4.4 Business Continuity/Disaster Recovery Tests

Central IT will conduct BC/DR testing using the approved DR contract. BC/DR test planning relies on the following approach to enable testing success:

- **BC/DR Testing Templates:** To address a thorough sampling of operational components
- **BC/DR Test Metrics:** Tier I metrics analyze the basic underpinnings of a BC program. Tier II metrics are more detailed and granular, and address data protection and recovery
- **BC/DR Testing Strategies:** To include build to recovery testing, verifying that the right people and processes have been identified for recovery testing, and deploying solutions
- **Cost Effective BC/DR Testing:** To include eliminating noncritical assets and processes

Disaster recovery testing best practices dictate regular, consistent and thorough testing utilizing testing tools when applicable. Disaster recovery testing tools fall into numerous categories including communications, replication, and automation and depend on the specific environment (UNIX, Linux, etc.).

The BC and DR Plan will be tested in order to validate their accuracy. All discrepancies will be addressed and the plans modified accordingly to accommodate any shortfalls. The security and availability aspects will provide guidance such as journalizing or documented recovery procedures to mitigate risks and avoid service outages. Rigorous testing of all recovery procedures included with the delivery of the solution will be performed prior to the introduction of a live system. Central IT will have copies of software as well as documentation, operating instructions, and recovery instructions filed at its remote site.

Central IT will perform a full test of the BC and DR Plan, and will report the results to the central IT and agency stakeholders. In addition to testing, the team will conduct a desktop simulation of the BD/DR procedures alternating with the complete test. A dry run will be conducted periodically by the IT staff, applicable users, and vendors to test the recovery platform. This testing can be done anytime as replication allows this without production environment impact. Various aspects of DR testing will be prioritized. The most critical aspects of the operation will be the focus for full-scale testing, with secondary testing done in slow activity time windows. A post-mortem analysis will be conducted at the end of the testing cycle and will include applicable vendors to address lessons learned and areas for improvement. If a test is unsuccessful, a remediation plan will be developed and we will re-test once the remediation work is completed.

5.4.5 Business Continuity/Disaster Recovery Best Practices

The scope for business continuity and disaster recovery includes infrastructure, applications, process and people. Priorities for IT recovery will be consistent with the priorities for recovery of business functions and processes and will be developed during business impact analysis. IT resources required to support time-sensitive business functions and processes will also be identified. The recovery time for an IT resource will match the recovery time objective for the business function or process that depends on the IT resource.

Recovery strategies will be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware components (networks, servers, etc.)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (operating systems, electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

5.4.6 Business Continuity/Disaster Recovery Report

Central IT will present an annual report of all BC/DR events in the previous reporting year to the agency and central IT stakeholders. Not only will the report document the details of the event, including the date time and a full description of the event, it will also document the actions taken and the impact on the agencies‟ ability to provide services. The report shows the number of times the DR plan was used and discusses the effectiveness of its use in each instance. When the plan is activated, a description of the incident that initiated the situation is reported and analysis is made of the event to determine if changes to processes or procedures need to avoid the same event occurring multiple times.

The Annual Recovery Report reviews the events that occurred and assesses:

- Whether appropriate personnel and responders were contacted
- Were event recovery process and procedures initiated according to plan
- Impacts to environment and Infrastructure and Business Applications

- Were Emergency Operating Procedures followed and if so adequate
- Did Security Controls work as planned
- Were Return to Normal Procedures adequate
- Recommendations from lessons learned such as whether process and procedures should be revised or infrastructure upgrades are advised

5.5 Access Management - (Future Capability)

Central IT will provide a user authentication solution to provide risk-based authentication mechanisms including but not limited to digital certificates, PKI-USB tokens, and soft tokens. Central IT will be responsible for defining and maintaining authentication processes for various users based on role categories and access mechanisms. The authentication management platform will support username and password based authentication and coarse authorization for Web applications against numerous repositories including LDAP. The platform will also offer a host of secondary factors for token-based or possession-based authentication. This will enable central IT to consolidate a user"s identity across enterprise applications and the LDAP compliant directory and be able to manage them from a centralized location. The solution will also synchronize with other resources such as LDAP or Active Directory, systems, and applications.

The combined platform provides coarse-grained authorization and single sign on. Authentication strength is configured respective to a risk score for a particular session and resource requested, which takes into account information about the session (time of day, location, etc.), security posture of the end point, sensitivity of data requested, type of access requested, and role of the user, among others. Single sign-on will allow users to log into central IT-supported systems such as wireless internet, ERP, and Statewide email. The State of Louisiana Service Desk will provide authentication support services, including user creation, password resets, and user access role updates.

The access management solution will be comprised of a few completely integrated technologies, performing the following functions: 1) provision users, 2) authenticate users, 3) authorize users, and 4) audit. The objective is to reduce the overall administrative tasks and time required for central IT to make a user productive, from provisioning the necessary user accounts, to associating them to the proper access control mechanisms in place for authentication and authorization.

The access management system consists of the following components:

- Two-Factor Authentication
- Identity Manager
- Access Control Management
- Directory Services

Two-Factor Authentication
The two-factor authentication of the access management system will provide authentication, authorization, credential, user/device management and session management. The two-factor authentication will utilize connections with an LDAP deployment and secure database for credential management and session controls.

Identity Management

Identity management enables central IT to manage the entire life cycle of user identities across enterprise resources. The identity management consists of the following services:

- Automates user identity provisioning and de-provisioning.
- Enables central IT to manage the entire life cycle of user identities.
- Provides self-service functionality (e.g., password reset, user management, etc.).
- Provides delegated administration.
- Provides synchronization of identities between the directories.

Access Control Management

Access control management is the mechanism used to control user access to central IT resources. The access control management function provides:

- Identity administration and access control to applications and resources running in heterogeneous environments.
- Compliance with organizational, regulatory and cultural access policies.
- Single sign-on access to services and through to third-party Web applications and other internal central IT applications.

Directory Services

Directory services are central to the identity and access management strategy. Directory Services will:

- Store identity data for internal and external central IT stakeholders.
- Delivers up-to-date identity data to the components that require it.
- Use the LDAP compliant directory service in order to provide the scalability, flexibility, availability and security features needed to support identity services.
- Support distributed stores of identity data.
- Support virtualization of LDAP and AD directories so that users and applications see one view of the identity and access management across multiple repositories.
- Centralized user administration of AD and LDAP.
- Have no single point of failure for applications using the aforementioned protocols to access identity data; Directory Server supports an unlimited number of masters or read-only servers.
- Enforce compliance with information security policies and to make sure that only those with proper authorization have access to the information.

5.6 Problem Management

Central IT takes the Problem Management process very seriously because it understands that any unplanned downtime or any issue impacting users of the systems must be resolved immediately. Central IT also understands that problems are not scheduled, and the team must always be ready to resolve them as soon as they occur. Central IT will have continuous automated and manual event monitoring in place with alert triggers and automated notifications to signal that a problem has occurred. Central IT will also have a team ready to resolve the problem as quickly as possible. When an issue occurs, central IT will enact the incident and problem management procedures to resolve the problem to minimize disruptions of normal system processing.

The team will escalate problems according to the documented incident and problem management procedures so that the appropriate people are notified of a problem and the correct resources are in place

to help resolve the outage as quickly as possible. The team will be trained on the problem management and escalation procedures on a regular basis. The management team will supervise the activities of the staff to make sure the problem management procedures are being followed correctly by observing the activities of the staff and providing constant feedback on their performance. The management team will regularly and randomly rehearse the problem management process with team members to make sure the processes are well known and to reinforce training.

Problem Management

Through the event management procedures, central IT will monitor the health of the systems and immediately identify problems in the environment should they arise. Central IT will also be on the ready for any user reported problems that may occur and will address the problems as soon as they are identified.

When a problem is identified, central IT will immediately enact the incident management processes to resolve the problem as quickly as possible (depicted in the figure below). Central IT will communicate to the appropriate people that a problem has occurred, what the problem is, the scope of the impacted problem area, a description of who is working on the problem and any other information that will be helpful for IT stakeholders to understand the severity of the problem. After the initial diagnosis of the problem, if it is determined that the problem will not be resolved immediately, the team will begin working to implement a work-around to the incident to restore services as quickly as possible.

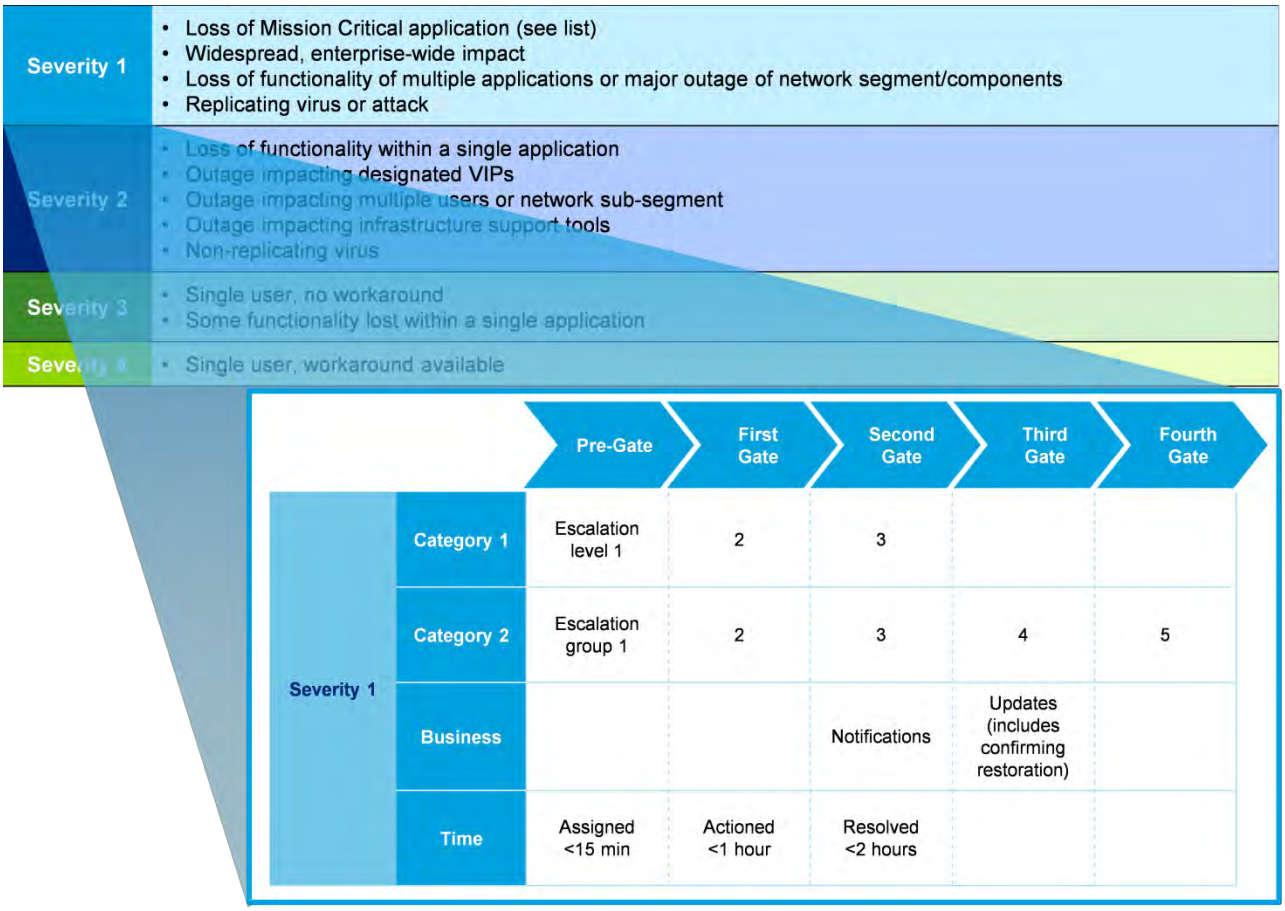

Figure 5.7.2. Problem Management Severity and Escalation Matrix.

Throughout the problem resolution process, central IT will have the right resources in place to minimize the impact of the issue and will be constantly communicating the status of the problem to keep users informed.

Problem Management Notification
Central IT will develop and implement ITIL based procedures for the problem management notification process. When a problem is identified, a Service Request ticket will be entered containing all of the information about the problem as documented in the procedures.

Once the problem notification procedures are invoked, affected users will be notified automatically of the time that the system became unavailable and when the system has been restored. There will also the updates for users to be notified of status of the problem if it is a prolonged outage.

The service desk solution automatically notifies a defined group of people when an interruption in service occurs either because of hardware, software, network or telecommunications failure. The system will notify stakeholders using the preferred methods of notification including email, and/or text. In addition, central IT can send a broadcast voice message to the departments that request that means of notification. Included in the procedures will be steps to invoke the problem management notifications using manual steps, in case the technology is unavailable to notify stakeholders automatically.

The procedures will include detailed steps to keep the notification distribution lists current. As resources move in and out of new positions there will be steps to add and delete names to update the notification lists. The distribution lists will also be set up so that the correct people will be notified for the problems they need to know are occurring. For example, a Level 1 complete system outage will notify the affected department staff identified as needing to be notified when a Level 1 outage has occurred. A Level 2 outage will only notify stakeholders on the Level 2 notification list. The notification will include information on exact time of outage, nature of outage, expected time to recover, and explanation of resolution in the notification to users. As part of the procedures the Systems Operations Dashboard will be updated with information about the problem as another form of communication. This will include the exact time when a problem occurred and the time when the problem was resolved.

5.7 Service Reporting

The Service Reporting process of the IT Operational Plan framework falls under Service Operation and is the process within the framework for reporting to stakeholders. Each of the various processes under the functional areas of the framework produces reporting data which is collected under the Service Reporting process.

The State of Louisiana"s Service Reporting approach focuses on three high-priority areas:

- Manage availability and perceived availability
- Performance
- Change management

The following subsections provide the objective, requirements, and the source of the data used to generate the report.

5.7.1 Systems Operations Report

Systems Operations Reports will be delivered by central IT to IT stakeholders and Customer Engagement managers from each customer department.

The Systems Operations Report will provide actuals versus targets, monthly comparisons and performance trends, as well as possible improvements and optimization measures that may be implemented. Results will include a graphical or presentation-style format.

Systems Availability
The objective of the Availability Management Report is to consolidate information in a manner that highlights the quality and effectiveness of the availability management process relative to service level targets. In the event availability achievements fall short of objectives, recommendations for improvements are also documented in the reports. The data used to produce the reports include information originating from the service requests or incident tickets. In addition to measuring service level availability achievements versus commitments, these data are used to understand trends and develop plans for future requirements.

The Availability Management Report includes:

- Actual availability data of critical components used to deliver IT services, including the UAT and training environments
- Servers summarized by each business function and environment
- Component failure data

Network infrastructure availability reporting provides:

- Summarized network events including network outages attributed to third-party telecommunication providers
- Central IT‟s analysis and explanation of all network events that impact systems availability and/or performance and status of corrective actions taken in response
- Summary report of all network-related software and patch update activities performed

The availability chart will be available for production, UAT, and training environments. Availability charts and supporting analysis will be included in the availability report section of the Systems Operations Report.

Central IT‟s availability reporting process will also capture the agencies‟ perceived view of the availability of systems based on information reported in service request tickets and the results of service desk customer satisfaction surveys. With this in-depth visibility, central IT can react more quickly to service degradation and restore service faster. Central IT will conduct periodic reviews of ticket information and survey responses related to availability, and provide analysis of the differences between actual and perceived availability. Central IT will track trends and, aligned with findings, make recommendations for

corrective actions to address any gaps. This constitutes a continuous improvement process, the goal of which is to progressively reduce the gaps between perceived and actual availability over time.

In addition to the information included in the Systems Operations Report, current systems availability information will be provided through an online information portal, enabling easy access to current information on any outages, along with the status of the outages and estimated resolution time.

The availability targets and achievements of each service level will be reviewed on a regular basis through the Customer Engagement process detailed in *Deliverable 14 – Customer Engagement Plan*. Testing the underlying service components‟ ability to achieve required service levels will be conducted periodically. The activity matrix shown in the table below provides a mapping of system availability activities, inputs, and outputs.

Monitor, Measure, Report, Investigate and Remediate			
Activity	**Inputs**	**Description**	**Outputs**
Monitoring Availability, Reliability and Maintainability of Components	• Availability/Recovery Designs • Availability Plan(s)	Availability Management will have provided the various IT operations teams with the parameters for monitoring. All teams, internal and external, should forward results to Availability Management in the manner and timing requested.	Monitoring Results
Measure Availability Against Agreed Targets	• Supplier Reports • Monitoring Results	Availability Management will have provided the various IT operations teams with the parameters for measures of Availability. All teams, internal and external, should forward results to Availability Management in the manner and timing requested.	Availability Analysis
Prepare Trend Analysis	• Monitoring Results • Availability Analysis • Incident Management Reports	Availability Management will correlate and analyze results of monitoring and measures and produce a Trend Analysis Report.	Availability Trend Analysis
Reporting	• Availability Analysis • Availability Trend Analysis	Reports will be compiled and distributed according to the accepted Availability Plan(s).	Required Reports
Investigate Underlying Reasons for Unacceptable Availability	• Problem Management Requests • Availability Analysis	During the course of analyzing results of monitoring/measuring, or as a result of Incident/Problem Management process activities, Availability issues may be discovered. Availability Management will work with Problem Management and IT operations teams to investigate reasons for unacceptable service Availability levels.	Remediation Solutions

Monitor, Measure, Report, Investigate and Remediate			
Is Immediate Resolution/Remediation Possible?	• Remediation Solutions • Availability Testing Results • Improvement Recommendations	A reason for unacceptable Availability has been discovered, or a case for improvement has been proposed. Is there an immediate opportunity to address the issue, or will the solution need to be incorporated into a longer term improvement program? Factors such as impact and cost will be factored into the decision making.	Decision
Provide Guidance and Assistance with Remediation	• Remediation Solutions • Improvement Recommendations	Availability Management shall contribute guidance and assistance to remediation efforts to address Availability concerns.	Remediation Efforts
Contribute Recommendations to Continual Improvement Program	• Improvement Recommendations • Remediation Solutions	Availability Management shall contribute guidance and assistant to continual improvement programs which address Availability concerns.	Improvement Efforts

Table 5.8.1.1. Activity Matrix of System Availability Activities, Inputs, and Outputs.

5.7.2 Systems Performance

The objective of the Performance Report is to provide information on capacity, utilization trending and other aspects impacting performance to service providers as well as customers and users, which can be used to demonstrate the achievement of service targets and as input to service level review meetings. The report focuses on comparison between required and actual performance and performance trends over time.

The source of the data for the Performance Report comes from monitoring and event reporting tools employed by central IT.

Central IT will include within the Systems Operations Report a summary of systems performance including, but not be limited to:

- Summary report of performance of systems online functions for each department as required by SLAs
- Summary report of performance of systems batch functions as required by SLAs
- Summary report of performance against all other SLAs
- Detailed report of CPU utilization, network bandwidth consumption, and data storage usage
- Top 10 slow transactions per system
- Top 10 transactions recently tuned
- Aggregate data in support of each summary report
- Central IT"s analysis and explanation of any performance incidents and plans for corrective action(s)

5.7.3 Operations Change Management

Consistent with central IT"s approach to operations reporting, change management reporting is an output of the Change Management process as part of the IT Operational Plan framework

The objective of the Change Management Report is to review the change process for efficiency and effectiveness, identify trends, and audit for compliance. The framework recommends reporting successful changes as well as changes that may have caused incidents. This provides an indication of the effectiveness and quality of the change management process as well as good input into the Quality Assurance area for application development and testing.

Central IT will include in the Systems Operations Report an Operations Change Report that includes a standard change report as well as the specific reports requested by the customer departments:

- Number of change requests implemented in the period in total by service and by CI
- Detailed description of all change management activities
- Listing of successful change requests
- Listing of change requests backed out of, and back-out reasons (i.e., incorrect assessment, poor build or fix)
- Listing of implemented change requests that were not successful and why
- Listing of pending change requests and a description of all incomplete activities carried over from previous months
- Listing of change requests per status with details of each activity and a current status and planned completion date (i.e., not assessed, assessed, approved, in process, pending)
- A forward schedule of changes with the activities to be performed in the next month

The source for the data used to create the operations change management reports comes from requests for changes along with incidents tickets in the central IT ITSM system.

The figure below provides an example of a change report listing the change number, the scheduled start and end date and time, the status of the change, and a summary description. The detailed description is not included in the graphic but is included in the production report. This report is used for reviewing changes at the Change Advisory Board (CAB).

Client CAB Report (Next 2 Weeks)
Friday, Feb 22 - Sunday, March 10, 2013
Report Run Date & Time: 2/19/2013 4:30:00 PM

Client Changes					
CAB Date	Change ID	Scheduled Start Date (EST)	Scheduled End Date (EST)	Status	Summary
2/25/2013	CHG0000000204XX	02/26/2013 19:00	02/27/2013 01:00	Approval Required	XXX- Additional SAN to PHX-XXX-LDS21/22.
	CHG0000000205XX	02/28/2013 14:00	02/28/2013 16:00	Approval Required	XXX C:D Node Change
	CHG0000000204XX	02/28/2013 14:00	02/28/2013 16:00	Approval Required	XXX: UPDATE CITI VPN TUNNEL CONFIG ON XXX VPN DEVICE
2/19/2013	CHG0000000204XX	03/03/2013 00:00	03/03/2013 06:00	Approval Required	Create a 310 Gb datastore and Consolidate the VMs on the XXX ESX cluster. Add vdisks to requested Linux VMs
2/19/2013	CHG0000000204XX	03/05/2013 17:00	03/05/2013 22:00	Approval Required	XXX - add additional disk space and grow rootvg on phx-XXXlfs21.
2/11/2013	CHG0000000191XX	03/09/2013 23:01	03/09/2013 03:00	Approval Required	Please install an LDAP 6.3 on PHX-XXX-LFS21 port 498
12/10/2012	CHG0000000195XX	03/10/2013 00:01	03/10/2013 06:00	Approved	UNRACK XXX DECOMMISSIONED P570'S
Shared Infrastructure Changes					
None					
	Interactive Users will be impacted	2 Week Lead Time			

Figure 5.8.3.1. Sample Change Report with Activity Details, Current Status, and Planned Completion Date.

5.8 Request Fulfillment

Request fulfillment, also known as the Service Request Management process, is responsible for managing the lifecycle of all service requests from authorized customers and within the scope of central IT.

Service Requests cover requests for server, mainframe, storage, network, security, and end-user device provisioning, as well as requests for IT services in the Service Catalog described in *Deliverable 10 – IT Service Catalog*.

The Service Request Management process provides the following key benefits:

- Ensures that service requests are classified and documented appropriately
- Reduces operational impact of service requests through timely fulfillment
- Improves customer productivity by quickly fulfilling requests

Severity
Severity is used to describe the impact of the service request on the customer. As a ticket is created, the State of Louisiana Service Desk analyst will assign a level that will then be reviewed and validated by the IT Supervisor and becomes part of communications with the customer.

Roles

The State of Louisiana Service Desk will have dedicated staff trained on the IT Service Catalog offerings, including service procurement, infrastructure provisioning, and end-user device procurement. Service Requests will be submitted through the Service Desk application to enable tracking and classification of requests.

Customers can contact the State of Louisiana Service Desk via phone or web to discuss service offerings through the IT Service Catalog. Orders can be placed through the Service Desk once the appropriate approvals have been met. The Service Desk staff are responsible for contacting central IT infrastructure and end-user support teams as necessary to complete the procurement process and close the Service Request ticket.

Process Flow

Central IT will develop a complete Service Procurement Process Flow to determine the process flow and handoff procedures for service procurement through the State of Louisiana Service Desk. The Process Flow will detail all steps and parties required to service each type of request, including service procurement, infrastructure provisioning, and end-user device procurement.

5.9 Capacity Management

The Capacity Management process is used to project future demand, predict required capacity, and address capacity gaps to minimize service disruptions for central IT services. The Capacity Management process implemented by central IT establishes open communication between agencies and IT about upcoming business demands and where there might be capacity constraints to be remediated. This process enables the organization to shift its attention from fighting fires to proactive planning for capacity management.

Area	Benefits
End-to-End Process	• Develop an enterprise level end-to-end process with clear roles and responsibilities and operationalize a quarterly cycle for the process • Collect and receive sign-offs on demand projections from agency and IT Owners of applications on a quarterly basis • Create a capacity plan that collects, consolidates and tracks to closure all capacity remediation action items from agency and IT stakeholders
Critical Agency Applications	• Identify applications for capacity planning with agreement from agency and IT leadership • Develop application demand models for applications that include identifying demand metrics including peaks, finding correlation between agency and IT metrics and adjusting for variance by comparing actuals to projections on a monthly basis

Application Infrastructure	• Develop capacity models for a portfolio of key applications across network, mainframe, and server platforms • Proactively identify capacity constraints early, which allows infrastructure teams time to procure and configure devices to handle peak volumes
Network Infrastructure	• Modeling of network resources and identifying network constraints provides IT the evidence required to receive funding to upgrade the network load balancers and head ends • Identification of the upcoming network bandwidth shortfalls allows for successful bandwidth upgrades months prior to peak load

Accurately managing capacity requires four steps, each described in detail below:

- Identify and Engage Stakeholders
- Project Future Demand
- Predict Required Capacity
- Address Gaps

Identify and Engage Stakeholders

The first step in central IT‟s Capacity Management plan is identifying all stakeholder groups that play a critical role in capacity planning. Each group must be accountable for their input to the process. The following are the key roles for the Capacity Management process:

Stakeholders	Responsibilities

Capacity Planning Team	• Manage the Capacity Planning process
	• Act as liaison between:
	  ○ Business and IT owners
	  ○ IT Application and Infrastructure teams
	• Create and manage the Capacity Plan

Agency Application Team, including Key Users	• Provide business demand projections • Receive regular updates on capacity planning progress • Justify variance in forecasts, adjust projections as needed • Sign-off on business projections
Central IT Application Teams	• Develop application transaction projections • Work with IT Infrastructure Team to assess capacity impact • Implement code changes (as needed) to identified in the Capacity Plan • Sign-off on applications‟ ability to scale to support projections
IT Operations / Infrastructure Team	• Receive and review application volume projections • Identify remediation needed in the infrastructure to meet projected demand • Implement infrastructure changes identified in the Capacity Plan • Keep infrastructure inventory current after each upgrade

Project Future Demand

End-to-end capacity planning requires collection and consolidation of agency and IT demand projections to properly understand the capacity requirements. Central IT will facilitate these projections by hosting regularly scheduled discussions with the identified stakeholders to accurately project and plan capacity requirements. The discussions will focus on three key processes: identify demand metrics, model application demand, and project application demand.

- **Identify Demand Metrics**: Central IT will work with stakeholders to identify the most critical metrics for the business baselines for each application requiring capacity planning. The group will identify the business and application demand metrics for each critical in-scope application.
- **Model Application Demand**: Central IT will obtain historic business and application actuals including peak volumes for the identified metrics. To develop Demand Models for the applications, the group will use the actuals to correlate application against business volumes and peaks. The business and application projections can then be calculated using the business baselines.
- **Project Application Demand**: After calculating the application and business projections using the business baselines, each stakeholder will then confirm and sign-off on the volume projections. Finally, the projections can be compared to historical volume predictions to calculate a variance to be applied to the new projections.

Predict Required Capacity

To best predict required capacity, central IT correlates between components of a system with user activity as the primary driver for resource consumption. This process focuses on three key processes: identify resources, model capacity consumption, and project usage and load.

- **Identify Resources**: Central IT will identify load and resource consumption information for each component of the critical in-scope application.
- **Model Capacity Consumption**: First, central IT will gather and analyze historical load and resource consumption data for the identified resources. Then, central IT will correlate the business and application volumes calculated in the previous process against the resource consumption. This will allow IT to identify and extrapolate trends and identify capacity thresholds.
- **Project Usage and Load**: Once capacity has been modeled, central IT can estimate the target utilization using the load forecasts. If any capacity issues exist, central IT will coordinate with the Capacity Management stakeholders to determine appropriate action items.

Address Gaps

Addressing gaps is also a 3-step process: Identification of action items, track action items to closure and confirm readiness. Action items are identified from capacity modeling and from agency and IT stakeholders and consolidated into a capacity plan.

- **Identification of Action Items**: In conjunction with the final step of the Predict Required Capacity process, central IT will work with Capacity Management stakeholders to identify action items to address capacity concerns. These action items will be determined by analyzing modeling trends and identifying capacity gaps. The action items will be consolidated into a capacity plan with respective action owners and timelines.

- **Track Action Items to Closure**: The Capacity Planning team will work with all action owners to obtain status of action items on a daily basis and escalate risks related to action item status/closure to senior management. Once the action item owner has confirmed that the task is complete, the Capacity Planning team will close the action item in the tracker.
- **Confirm Readiness**: Once action items have been closed, the Capacity Planning Team will reach out to agency and IT stakeholders to confirm application readiness from a capacity perspective. The team will then finalize a readiness confirmation report to be provided to the Capacity Management stakeholders and central IT management.

6.0 Technology and Infrastructure Management

The Technology and Infrastructure Management process includes the technology, infrastructure, and application services and policies to operate the State of Louisiana systems.

6.1 Technology Operations

The Technology Operations process in the IT Operational Plan Framework includes the facilities, servers, equipment, network, and service desk provided by central IT.

6.1.1 Facilities

Central IT will provide and maintain the enterprise data centers for the State of Louisiana. Central IT will operate the managed services procured by customers from the primary data centers. The Facilities approach is detailed in *Deliverable 16 - Facilities Strategy and Management Plan*.

The Central IT facilities strategy includes two primary data centers in the Baton Rouge area: ISB and DPS. The two provide data center facilities with characteristics of Tier II data centers, as rated by the Uptime Institute. The data centers host State and agency systems, network, and technology equipment.

Data Center Model
The two data centers serve as primary and secondary data centers for systems to run and operate the State of Louisiana technology environment. Applications are built with one of the data centers as primary, with replication and failover architecture available in the alternate data center. To avoid customer confusion and other problems, it is critical that both data centers have the same chargeback rate and policies for floor space and electricity.

Central IT will continue to improve the reliability of the data centers and progress towards Tier III characteristics at both ISB and DPS. A data center with Tier III capabilities has redundant capacity components and multiple independent distribution paths serving the computer equipment. Typically, only one path serves the computer equipment at any time. IT equipment will be dual powered and installed properly to be compatible with the topology of the site"s architecture. Each and every capacity component and element in the distribution paths will be able to be removed from service on a planned basis without impacting any of the computer equipment, but an unplanned outage or failure of any system may impact the availability of the systems. Planned site infrastructure maintenance can be performed using the redundant capacity components and distribution paths to safely work on the remaining equipment.

Data Center Layout
Central IT will begin to use leading practices for data center layout. This includes using Performance Optimized Design (POD) principles for the incremental build-out of the data center floor space using standard components and practices across the data centers. A POD is a set of defined computing,

network and storage resources that can be designed with expandability options for computing and storage. Overall, POD designs provide tighter integration and better standardization for data center operations. Power zones provide a range of power density and cooling depending on the application/computing requirements for each POD. Component configuration optimizes power and cooling by zone. The POD design philosophy will lead to the following benefits:

- Increased flexibility and improved ability to adapt to changes in demand
- Reduced up front investments and improved operating costs by up to 40%
- Enabled effective utilization of resources and minimized waste by minimizing over provisioning
- Repeatable and scalable; with reduced lead time for adding new capacity

Power

To support the existing and future infrastructure at both primary data centers, central IT will implement redundant power paths to all systems. Failure in any single point in the power supply chain will not result in system outages. This includes redundant and fault-tolerant UPS, backup generators with fuel, and diverse power carriers entering the data center at diverse points.

Future power requirements will be calculated using the process detailed in *Section 5.10 – Capacity Management.*

Power consumption will be reduced through central IT sustainability efforts. Virtualizing server platforms will consolidate workloads on fewer servers, allowing for more efficient power and cooling. Application rationalization will reduce the power and cooling costs by consolidating disparate systems. Finally, migrating servers to the third-party cloud provider will further reduce power requirements.

Monitoring

Systems will be monitored by central IT using the central monitoring tool described in *Section 5.1 – Event Management.* The monitoring will include thermal readings, availability, performance, and capacity. Alerts will be triggered whenever any defined threshold is met, resulting in an automatic ticket creation in the State of Louisiana Service Desk solution. This will automatically notify facilities and/or infrastructure support staff of any erroneous activity in the data centers.

Physical Security

Central IT will provide security controls for data center access. Leased floor space in both data centers will be kept in locked cages to prevent unauthorized access. Access into each data center will be provided only to approved facilities personnel and customer defined access lists maintained by central IT. Security guards will be stationed at data center entrances at all times, and all entry into the data center will be monitored and recorded. Closed circuit TV surveillance and DVR service will allow for continuous recording of the data center.

Fault Tolerance

Reliability of data center systems and components is measured in terms of availability. Central IT will use leading design practices involving redundancy and bypass components to maintain service during disruption and maintenance. Electrical and mechanical distribution systems consist of a chain of

equipment and components, so failure of a single item can result in an outage unless redundancy and/or bypass is provided.

Central IT will use a fault-tolerant design to eliminate single points of failure. A single point of failure is considered any single component, which in a failed condition will inhibit the operation of the data processing operation. From the standpoint of electrical power distribution, it is any item that delivers power to the data processing equipment or to the environmental support equipment that maintains the temperature and humidity control of the data center. Without power to the environmental support equipment, the computer hardware will be susceptible to thermal shutdown. On the mechanical side, it is any component that delivers or provides the cooling for the data center environment, electrical distribution equipment rooms, and computer hardware.

To qualify as a single point of failure, the components identified will meet one of the following criteria:

- **Single Device**: Where the failure of the device can completely disrupt the data processing operation.
- **Single Route**: Where there is only one physical path existing between geographically diverse equipment.
- **Co-located**: Where redundant/alternate components reside together.

At an application level, central IT will provide high availability across the primary data centers. This process is detailed in *Section 5.3 – Availability Management*.

Disaster Recovery and Business Continuity
For disasters affecting both primary data centers, central IT will procure a consolidated disaster recovery contract with a geographically diverse third-party provider. The disaster recovery and business continuity planning is discussed in detail in *Section 5.5 – Service Continuity Management*.

6.1.2 Servers, Operating Systems, Equipment, and Network

Central IT will provide, install, maintain, and manage all hardware, operating systems, security software, and third-party software associated with the enterprise servers and associated peripheral devices.

Network Strategy
Future state network strategy and policies are documented in *Deliverable 17 – IT Network and Communications Plan*.

Operational Support
Central IT"s approach to the operation of the enterprise servers, along with the processes and procedures that prescribe how IT will perform the tasks associated with operational support, are guided by the IT Operational Plan framework. Some key features of our operational support include:

- **Server Hardening**: Central IT will perform hardening on all enterprise servers based on industry standards and following the standard procedures defined in the framework. This provides up-to-date compliance with industry-recommended settings throughout the State"s environment. Industry standards are updated (following the change control process) as new potential threats

are identified and remediated. This allows Central IT to respond rapidly to changing technologies and threats before they impact the departments, and to follow industry best practices from an audit compliance perspective.

- **Server Builds**: Central IT, as part of the initial server implementation, creates a server build book. This book is documentation designed to provide operations with an accurate account of all configuration settings needed to bring a server to its Production state, including any subsequent configuration modifications made as a result of vulnerability assessments and other security hardening efforts.
- **Anti-virus**: Central IT includes and mandates that anti-virus support is maintained on all supported servers. Monitoring and updates are provided according to central IT"s anti-virus support process.
- **Asset Management**: Asset management is an important component of the IT Operational Plan Framework and is provided by central IT with a complete Change Management Database (CMDB). The CMDB contains the equipment hardware information, Internet Protocol (IP) configuration, Operating System (OS) level, rack location, and support and licensing agreements. The CMDB is updated with every subsequent change as part of the change management process defined in the framework, and described below. The CMDB provides a Configuration Item (CI) to link to the server build book for detailed documentation of each server implemented and managed by central IT.
- **Change Management**: Change management is another important component of the IT Operational Plan framework that regulates the changes to the environment and provides stability and predictability of performance. Regular changes and emergency changes follow the change management process, which includes approval from the Change Advisory Board (CAB). The CAB reviews testing results, back-out plans, client notifications, documentation updates and risk mitigation. The CAB, upon approval, allows IT engineers to schedule updates to systems. Additional information on the Change Management process is provided in *Section 4.1 – Change Management*.
- **Patch Management**: Patch management refers to the acquisition, testing, and installation of patches related to the vendor"s operating system and base components. Server operating systems provided by vendors are fundamental components of servers. Vendors release patches based on both a regularly scheduled release window as well as an ad hoc basis. These patches assist in minimizing and/or eliminating potentially dangerous exposures within the operating systems, therefore stabilizing and reducing the risk of intrusion and/or malfunction. The patch management process defines a regularly scheduled implementation of all levels of fixes and patches relevant to the environment. This facilitates a controlled release of fixes and patches, which are monitored and reviewed by central IT. The patch administrators analyze individual servers to determine which patches must be acquired and installed to comply with organizational standards.
- **Firmware Updates**: Firmware updates are provided in an agreed-upon schedule, according to the change management process. Firmware updates are almost always recommended by vendors to maintain the support agreements. Central IT will apply firmware updates when needed utilizing the change management process.

Technology Refresh

Keeping users on current technology is important to delivering high levels of service to end-users and keeping maintenance and support costs down. To maintain the stable and performance-tuned

environment, central IT monitors the support timelines published by the original equipment manufacturers (OEMs) and initiates refresh planning projects at least a year in advance of published end of service announcements from an OEM.

Capacity Management
Central IT maintains current baseline system performance and resource capacity. During testing of modifications or enhancements to the system prior to their implementation into production, central IT monitors the pre-production environment and performs analysis with the current baseline. Based on the analysis, central IT determines if the existing resources and tuning of the system are sufficient to proceed into Production. If not, then prior to promotion of any modifications or enhancements, the lacking resources are identified and resolution steps are performed.

Central IT also performs capacity planning in a steady state for the production environment. This includes tracking current capacity levels for IT assets and developing trend lines of utilization. Central IT will make management aware of the need for new IT infrastructure purchases before capacity limits are exceeded.

Enterprise Systems Servers Management
Central IT will perform monitoring of the enterprise servers for equipment, software, and performance problems. Should the monitors detect conditions that could impact meeting SLAs, the monitoring system will then create an actionable event in the monitoring system that first implements automated operational actions, if possible, to resolve the impending event. In parallel, the monitoring tool opens an event ticket that is assigned to the appropriate server engineering team to inspect and manually resolve the problem, if necessary.

Desktop Images
Central IT will maintain standard desktop images for standard State of Louisiana end-users. These images will be available for imaging new end-user devices as well as re-imaging devices when necessary. The images will only contain standard State of Louisiana systems, applications and virus protection. Agency specific applications and other applications can be added according to the Services Catalog.

Process
Change Management is responsible for the smooth coordination of all software updates, especially during crucial planning and preparation stages, and is closely involved with Release Management. Change Management co-ordination means that approvals have been received, communication has been sent to all stakeholders, documentation and training have been provided to technical support staff and end-users, risks have been mitigated, and operations is prepared to implement the change in the live environment.

Using the Change Management process, central IT will notify the departments of the impact of any software upgrade to the operations of the systems prior to upgrading the software.

Central IT will work with all vendors and will leverage vendor partnerships so that State of Louisiana software is fully supported. Central IT adheres to the Change Management process for all environmental changes, including in-scope software support. Security and anti-virus software components for all environments and devices will be updated regularly, with the latest software, patches and anti-virus definitions available from the manufacturer unless otherwise accepted by the agencies.

Central IT will procure and manage the licenses, maintenance contracts and upgrades for the software components of the solution, including the annual maintenance of the database licenses. The software components shall include:

- Operating system
- Database system
- Middleware software
- Data encryption software
- Open source software
- Document management tools
- Terminal emulation tools
- Secure file transfer tools
- Network management control system
- Performance management and measurement tools
- Management report tool
- Local office server tools, including:
    - Local management reporting
    - Local management content on demand
- Service desk application
- Change request tracking application

Third-Party Software Component Upgrades
Central IT will provide services required for upgrading the software components of the systems including:

- Impact analysis
- Planning
- Design
- Testing
- Implementation

All upgrades will go through the established Project Management Change process for quality assurance and completion of component tasks as listed above.

Acceptance of Software Upgrade Exception
Under special circumstances, central IT may request an acceptance of software upgrade exception. Typically requests to upgrade software are made to take advantage of new features that could benefit the productivity or performance of the environment. In such cases, central IT will direct exception requests to the departments using the Change Management Process described in *Section 4.1 – Change Management*. The request shall include specific details about the reason for the exception request and plans for future software upgrades.

Software Maintenance Agreements
Central IT will procure and manage maintenance agreements for software components within the central IT environment, and renew them as needed throughout the term of the agreement.

Central IT employs a centralized approach to software license management in conjunction with asset and configuration management. Using the CMDB Asset Management component, the process tracks software licenses throughout their life cycles from planning through acquisition, maintenance, and disposal. This facilitates the evaluation of business plans and computing requirements during the planning period before procurement decisions are made. The process also provides financial data management and contract management using lease management and third party contract and license tracking.

Software License Management prevents software purchases from being made before their impact is tested in the environment. It also confirms that detailed purchase records are maintained so that IT expenditures are accurately reported on corporate financial management records.

Software License Management also contributes to the maintenance of the product catalog by determining that purchases are made against a standard contract. It helps develop, monitor and enforce corporate governance, data security and provisioning rules surrounding the procurement, maintenance and retirement of assets.

Central IT will procure a higher level of support as needed for the contracted SLAs if it is determined that a higher level of support is required to achieve and maintain SLA compliance.

In the event that commercial maintenance is unavailable for any software included in the solution environments, central IT will notify the affected agencies.

6.1.3 Service Desk

Central IT operates the State of Louisiana Service Desk for service incidents and service requests. Central IT‟s approach for providing the service desk capabilities is to provide a single consolidated capability where incidents and service requests can enter the Service Management process. This capability provides an effective set of information management processes and controls and describes the way information systems and IT service activities are provided.

In the Operations Framework, the service desk is described as a function of the technology management processes. Within this function, the service desk executes the incident/problem management, request management, and escalation processes. Aligning with industry leading practices, the service desk owns all requests and oversees their disposition throughout their lifecycle. Although the Service Request (SR) ticketing system provides automated escalations, the service desk owns the requests and follows up with the groups assigned to them to avoid missing the service level goal.

Technical Function and Support
The State of Louisiana Service Desk, provided by central IT, will provide two communications channels for customers to use in reporting incidents/problems and questions/requests: telephone and the Service

Request (SR) portal via the web. The technology that is used for entry of SRs is an integral part of the integrated IT service management capabilities that will be used to support the State of Louisiana"s environments and users.

The service desk will be available by phone 24 hours per day, 7 days per week (including holidays) and the customers can always contact a live person when calling for support. An automated call distribution system will route customer calls to an appropriately skilled central IT help desk staff. The Service Desk Team supporting the State of Louisiana Service Desk will be trained on the service desk application, the overall State environments, and the use of the systems. Central IT will identify common requests and incidents that can be resolved by the service desk. Appropriate scripts will be developed and added to the knowledge base to address the most common incidents and requests. The knowledge base is accessible by the Service Desk Team staff. The service desk manager will work with the technical and functional managers to continuously identify requests and incidents that can be resolved by the service desk.

In situations where the service desk cannot resolve the request or incident on first contact, the ticket will be assigned to an appropriate group. When the request or incident is determined to be an urgent deficiency, the service desk assigns the ticket to the appropriate group and also makes a phone call to the appropriate systems developer, policy support analyst, or quality analyst to verify that they have received the ticket. After normal business hours, the service desk will contact the technical and functional support team if an urgent deficiency is reported.

Central IT is committed to meeting or exceeding the service desk requirements stated in *Deliverable 10 – Service Catalog*. Central IT understands that access to the service desk and its support operations is critical. Central IT will provide access for departments" designated users to systems and knowledgeable support staff. Service Desk support staff possesses the breadth of skills necessary to resolve issues and provide answers to questions on the use of supported State of Louisiana systems and to troubleshoot other technical problems the departments may encounter.

A user-friendly, effective service desk has a direct and positive impact on user satisfaction, confidence, and compliance. Central IT will use the technologies described in in the following table to provide the required coverage and access to our service desk and related support functions.

Tool	Purpose	Benefit to the Customers
Customer Satisfaction Survey	• Provides an independent industry standard measurement of customer satisfaction with service center	• Objective performance measurement including benchmarking against other companies and industry averages • Supports continual quality improvement
Automated Call Distribution (ACD)	• Provides call routing and reporting	• Promotes rapid response to callers • Provides metrics on calls for performance tracking

Tool	Purpose	Benefit to the Customers
(SR) Service Request Tool	• Request Management • Incident Management • Change and Release Management • Service Level Management • Reporting • Knowledge management repository	• Facilitates the request management process end to end • Automates escalations and assignments, where appropriate • Identifies potential SLA breaches before services are impacts • A variety of reporting options • Accurate, rapid responses to service center callers

Contacts to the service desk made either during or after business hours will follow well-established call routing, handling and reporting procedures. The associated Service Level Agreements are described in detail in *Deliverable 10 – Service Catalog.*

Central IT will implement a fully integrated ITIL-based incident management solution with appropriate levels of management and controls for identification, analysis, and rapid response. The method will integrate application and infrastructure requests as well as third-party requests to create a seamless incident management process for the State of Louisiana.

Central IT will provide incident and request management support using a SR tool, providing clear visibility into incidents and how they are resolved. This is accomplished by deploying and maintaining effective, integrated, automated support and monitoring and clearly identifying the urgency, impact, and priority based on State standards. This allows central IT to properly assess, classify, and allocate resources to resolve incidents. Central IT also provides appropriate communication to stakeholders at designated stages in the ticket life-cycle. This includes stringent monitoring of ticket activities and queues paying particular attention to SLAs for each of the ticket types as captured in the sections below.

Central IT will make an initial response to the originator of the ticket via phone call or automated email for production environment incidents reported to the service desk within the published SLAs based on ticket priority. The initial response will include an analysis of the problem and an action plan for resolution.

Incident Tickets Resolution

Using the SR Service Desk application, central IT will resolve incidents, requests, and problems reported to the service desk. Central IT will create ticket templates to help guide the resolver in filling out the ticket to meet the requirements. Central IT will document in the ticket a complete detailed technical analysis of the problem based on available information and the proposed solution to resolve the problem. If the problem is determined to be a Systems Deficiency, central IT will determine if it is a design, code or policy deficiency and initiate appropriate procedures to resolve it. If the problem is determined to be a systems design function, central IT will propose a solution and/or workaround to the problem.

Production Environment

Central IT"s approach to the service desk provides a single point of contact for the customers for both application and infrastructure requests. When operating system or other software-related production environment requests are reported to the service desk, central IT will resolve tickets based on the following criteria.

1. Priority	Definition
High	• Affects an entire site or a large number of users and no temporary solution or workaround is known
Medium	• Affects an entire site or a large number of users and a temporary solution or workaround is documented
Low	• Affects only part of the users at a site or a limited number of users and a temporary solution or workaround is documented

Incident Management
Incident Management is detailed in *Section 5.2 – Incident Management.*

Problem Management
Problem Management is detailed in *Section 5.7 – Problem Management.*

Service Desk Application
Central IT"s integrated IT service management solution will include an industry-leading service management tool, including a SR Service Desk module which will serve as the service desk application tool. The SR service desk module will facilitate the high visibility of incidents and help provide insights into how they are being resolved. The SR tool is a browser-based application that is intuitive and allows customers and departments to record new incidents, view the status of existing incidents, and update information of previously reported incidents. The departments" Project Staff and the departments" QA Project Staff will have access to view tickets based on their role.

Reporting
The SR tool will provide advanced search and ad-hoc reporting capabilities, facilitating searches and offering complex search criteria. Reports can be printed, emailed and downloaded in a variety of formats. Reporting is detailed in *Section 5.8 – Service Reporting.*

Audit
The SR tool will provide a unique identification number and time stamp for each request and incident. The SR tool will maintain historical records of updates made to the ticket using industry best practices. The best practice approach is to create a work log entry for each new comment rather than modify existing entries.

Each work log can be locked, if needed, to prevent updates after it is initially saved. A manager will be able to use the work log entry to better understand the events that took place during the incident to identify root causes.

For example, in the case of a server event, the manager can use the work log entry to better understand the events that took place during the incident for the customer, service desk, and server support group, and examine the root cause and the resolution.

Knowledge Management
The Knowledge Management process used by Service Desk staff is detailed in *Section 4.4 – Knowledge Management*.

Customer Access

Central IT service request management (SRM) self-service solution will provide a portal where customers can request available IT services, record new requests or incidents and specify urgency, view the status of and update existing requests, and attach files to a service request to assist in troubleshooting. The SR portal also will provide access to the knowledge database for research for solutions to common and known problems. When needed, customers will be able to record their analyses and maintain historical information and troubleshooting notes in the ticket using the SR portal.

A customer will be able to use the SR portal to submit a request to add a new user to the SR portal. The project team member will select “request a new user to the portal” from the service catalog, input the specific information required into the automated form and submit it.

Following a predefined workflow, the request will be automatically routed for approval, and the approver will be notified via email to approve the request. Once the request is approved, the request is routed to the appropriate assignment group to create the new access. Later, the customer can access the portal to check on the status of the request. If the event status is still pending approval, the customer can contact the approver to expedite the process, if needed. In addition, the request could also trigger a workflow to notify central IT that the new user requires training.

Categorization and Assignment

The SR Service Desk application will provide the ability to link and de-link individual service requests to issues, track individual service requests and issues that have multiple linked service requests. The SR tool will also provide the functionality for auto-assigning incoming service requests to specific analysts or groups based on type of incident and user-defined rules. These rules will be easy to create and modify.

The SR tool will provide the ability to auto-assign incoming service requests to specific analysts or groups based on type of problem and user-defined rules.

Additionally it will allow for different routing rules for different roles. For example, for a server incident in the State of Louisiana systems, the service desk support group is the owner of the incident but the server support group would be the workgroup assigned for resolution. In this case, different rules are created for the owner and for the assigned workgroup and workflow rules are applied accordingly.

Enforcement

Central IT will create templates in the SR Service Desk application to enforce system integrity rules that require users to enter certain minimum information on each service request. Requests and incidents will be configured to provide easy categorization of reported items.

As another example, to effectively communicate with the ticket originator, the Service Desk manager may require that the Service Desk application collect the ticket originator"s name, phone number, and email address and record it in the ticket. The Service Desk application will respond with an error if an analyst attempts to save a ticket without the originator"s name, phone number, and email address.

The SR Service Desk application will also be able to also enforce:

- Access and permissions to various features of the Service Desk application by roles and specific users

- Restriction of updates to closed tickets

Escalation and Notification
To meet escalation and notification requirements, the SR Service Desk application will provide the following functionality:

- Automated escalation of service requests based on defined rules
- Automated notifications to originating users as well as to users to whom the service requests are assigned whenever an update has been made to the service request and if the service request is escalated to the next higher level
- Broadcast capability to announce system notifications to users

6.2 Application Management

As part of the IT Operational Plan framework, the Application Management process includes application support, application improvement, user support services, and general services. Each sub-process includes responsibilities for central IT and application customers.

6.2.1 Application Support

Resolve Application Issues
One of the core responsibilities of the application support teams is to resolve application issues reported through the State of Louisiana Service Desk. Central IT will attempt to resolve application issues that State of Louisiana staff are experiencing. Support will either result in the issue being resolved through a work-around or clarification of how the technology should perform, or an enhancement request to provide the new capability.

Central IT will:

- Fix functional and technical applications errors. This may include one or more of – procedural workarounds, code changes, databases or other date structure changes or documentation and procedural changes.
- Maintain application code in a professional manner and in accordance with good industry standards regarding structure, naming conventions, clarity and readability. Conduct internal code reviews and walkthroughs of significant modifications where appropriate.
- Maintain application code under software change control and include in-code comments to facilitate maintainability of the code.
- Document changes to the application code as a result of a functional and/or technical application error fix.
  Facilitate out user acceptance testing on fixes.

Maintain Application Quality
In order to support a high quality application experience, User Group Meetings will be held on a regular basis for each critical application supported by central IT. Central IT and customer representatives are expected to participate to discuss application quality and service delivery. Requests for new or updated

applications will be held through the Customer Engagement process detailed in *Deliverable 14 – Customer Engagement Plan.*

Central IT will:

- Participate in quarterly application user group meetings and discussions.

Recover Application After Service Disruptions

Once service disruptions or planned outages occur, the application will need to be restored to end-users. Central IT will work to restore application services after a service disruption. If the disruption is a planned maintenance event Central IT will restore application services according to a pre-defined plan for service restoration. If the disruption is an unplanned event Central IT will follow the Incident or Problem Management processes to restore services as according to the priority and urgency requirements defined in those processes.

Central IT will:

- Recover application service to meet Service Levels defined.
- Application service recovery means recovering the service end-to-end – not simply fixing a failed component. It may include recovery and repair of data (to the extent reasonably practicable), restoration of production services, working with customer and Third Parties and any other corrective or work-around action required to eliminate or minimize the business impact of the service degradation.

Database Administration

For supported applications, central IT database teams will support all databases and associated data. Central IT will support databases to make sure they are performing according to the application expectations. This will include tuning for performance and managing the space of the databases within the constraints of the storage capacity.

Central IT will:

- Maintain, optimize and organize databases and associated data structures and their definitions so that applications will meet the Service Levels.
- To the extent reasonably practicable, monitor the performance of databases to support applications performance and make recommendations for performance improvement. The implementations of any recommendations shall be implemented through the Change Control Process.
- Use all reasonable care and attention to maintain the integrity of databases and other file structures.
- Use all required security procedures for sensitive data.

Data Archiving, Deletion, Retention and Retrieval

For applications that require it, central IT will archive and manage legacy data. Central IT will perform data archiving, deletion, retention and retrieval services according to the procedures set in the State of Louisiana data management policies.

Central IT will:

- Carry out data archiving, deletion and retention activity on a periodic basis to meet Service Level Agreements.
- On customer"s request retrieve archive data in a controlled manner so as not to impact daily operation.

Technical Consultation
Central IT will provide best-effort technical consultation to end-users upon request. Technical consultation requests are handled through the State of Louisiana Service Desk.

Central IT will:

- Provide technical advice and consultation on user request.
- Provide technical or procedural workarounds as necessary, unless the Service Provider notifies customer as soon as possible that this is not reasonably practicable.
- Provide technical consultation and support required for end user computing.

Data Resource Management
Central IT will maintain data and other resources for supported applications. Central IT will also provide Data Resource Management consulting services to end-users through the State of Louisiana Service Desk.

Central IT will:

- Maintain data dictionaries and necessary meta-data.
- Advise users and make recommendations regarding data field location, recommended usage, availability and standards, including coding structures.
- Assist customer in a timely manner on the impact of any data protection legislation or other regulatory issues arising from current or proposed data usage.
- Maintain the data resource needs generated by end user computing.
- Use all reasonable care and attention to prevent corruption to the data.

Desktop Client Support
Several applications require thick or thin clients installed on end-user workstations to enable application access. Central IT will support the client application software for State of Louisiana staff as needed.

Central IT will:

- Support applications operating on the desktop platform including client components of client/server applications.
- Carry out modifications to these applications necessary to ensure they function under new releases of the desktop.
- Acceptance test these applications and application components if necessary, as part of upgrades to the desktop platform.

Support Development and UAT Environments
Central IT supports Development and User Acceptance Testing (UAT) environments for software development and end-user testing. Development environments will be made available to create enhancements to applications or develop new applications. UAT environments will be created to provide the ability for end-users to test applications before they are deployed into production. The UAT environments may not have the full capabilities of the production environments given budget constraints. Every attempt will be made to provide the most accurate testing environment given the constraints of existing infrastructure services.

Central IT will:

- Maintain a controlled environment which allows applications support staff to conduct user acceptance testing in a controlled manner for application fixes, modifications, improvements and other systems changes where acceptance testing is agreed upon. This environment should not allow further change by applications support staff to be made to application fixes, modifications and improvements once these have undergone acceptance testing and approval. No applications support staff may make changes directly in the production environment.
- Implement a formal software release and control process to promote software changes to the production environment.

Software Release Management
In order to support smooth software releases, central IT will follow the software release processes detailed in *Section 4.3 – Service Testing, Release, and Deployment Management.*

Central IT will:

- Operate a process for implementing new software releases.
- Analyze the impact of all proposed new releases and seek approval prior to implementation. The Service Provider shall propose, on a case by case basis, whether upgrades are „major" and should require acceptance testing, and then agree the status with customer.
- The Service Provider shall carry out user acceptance testing based on the availability of a user acceptance testing environment and agreement with customer.
- Maintain a log of changes, fixes, patches and new features that are included within each new release – with each log record uniquely identifiable and auditable.
- For major releases agree through the Change Control process to schedule implementations of major releases in conjunction with customer and impacted third parties where these are potentially affected by the new release.

6.2.2 Applications Improvement

Another one of the core responsibilities of the application support teams is application improvement. Requests for major application changes are handled through the Customer Engagement process, as detailed in *Deliverable 14 – Customer Engagement Plan.*

Central IT Responsibilities:

- Make improvements to maintain and improve applications and make improvements at the request of customer. This shall include the following types of improvements:
    - **Adaptive**: Minor modifications to an existing application that allow it to operate in a changed environment. “Changed environment” refers to modifications in hardware, operating system, compilers or system utility upgrades that impact the performance or operation of the application.
    - **Preventative**: Minor modifications to applications that make them easier to maintain or reduce the likelihood of future problems. This includes applying vendor patches, fixes and upgrades as needed.
    - **Mandatory**: Limited work effort associated with mandatory improvements covering health/safety, environmental, legal, tax and regulatory changes. These mandatory improvements are those which are deemed to be necessary by customer for the continued operation of its business.
    - **Discretionary:** Minor enhancements of applications. These would be minor modifications to an existing application that enhances current functionality.
- For the avoidance of doubt this shall include:
    - All functional modifications and improvements
    - All new data interfaces and reports
    - New interfaces, business process changes etc.
    - Help to analyze and specify new requirements
- Carry out user acceptance testing on improvements.

6.2.3 User Support Services

Central IT will support users who contact the State of Louisiana Service Desk. More details can be found in *Section 5.2 – Incident Management* and *Section 5.7 – Problem Management.* Central IT will also be a source of support for technology solutions for State of Louisiana staff who can contact central IT through the State of Louisiana Service desk. The Service Desk will attempt to provide support for application and end user devices to help staff utilize technology more effectively.

6.2.4 General Services

These service elements are to be delivered in relation to all parts of Infrastructure, Applications and User Support and shall be deemed to be a part of all such Services for the purpose of such service definitions.

Service Disruption Notifications
Service Disruptions will be sent out to all impacted users upon problem detection and resolution. The process for Service Disruption Notifications is detailed in *Deliverable 14 – Customer Engagement Plan*.

Availability Management
Availability Management is detailed in *Section 5.3 – Availability Management*.

Customer Relationship Management
Customer Relationship Management is detailed in *Deliverable 14 – Customer Engagement Plan.*

Service Change Management

Service Change Management is detailed in *Section 4.1 – Change Management.*