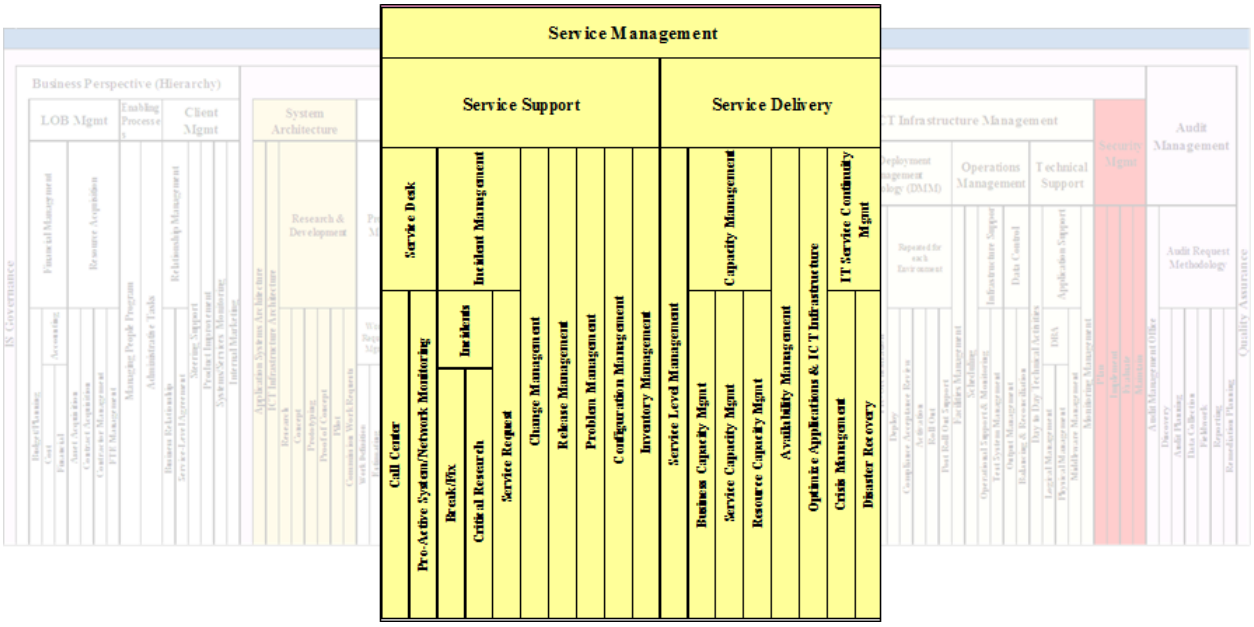
South Carolina

BlueCross BlueShield of South Carolina is an independent licensee of the Blue Cross and Blue Shield Association

imagination to Implementation

INFORMATION TECHNOLOGY

Service Management



Information Systems Standards Manual

Table of Contents

Table of Figures

List of Tables

Chapter 1 Service Management Overview

1.1 Service Management Governance

Chapter 2 Service Support

2.1 Incident Management

2.1.1 Incident Management Participation

2.1.2 Incidents

2.1.3 Break/Fix Incidents

2.1.4 Emergency Changes

2.1.5 Critical Research

2.1.6 Service Request

2.1.7 Contacting a Vendor about a Problem

2.2 Problem Management

2.2.1 Overview

2.2.2 Roles and Responsibilities

2.2.3 Problem Escalation

2.3 Change Management

2.3.1 Purpose

2.3.2 Change Flow

2.3.3 Change Management Meetings

2.3.4 Management Procedures and Responsibilities

2.3.5 Service Management Analyst Responsibilities

2.3.6 Change Management System

2.4 Release Management

2.4.1 Release Management Introduction

2.4.2 Release Management Process Overview

2.5 Configuration Management

2.5.1 Configuration Item Management

2.5.2 Introduction

2.5.3 Purpose

2.5.4 Policy

2.5.5 Objectives

2.5.6 Scope

2.5.7 Management Meetings

2.5.8 SharePoint Online

2.6 Inventory Management

2.6.1 Software Reviews

2.6.2 Software Compliance Audits

2.6.3 Infrastructure Hardware Cyclical Inventory

2.6.4 Infrastructure Decommission

2.6.5 Missing Equipment

2.6.6 Resource Acquisition Standards

Chapter 3 Service Delivery

3.1 IT Service Continuity Management

3.1.1 I/S Crisis Management

3.1.2 Disaster Recovery Program Overview

3.1.3 Disaster Recovery Program Onboarding

3.1.4 Disaster Recovery Plans

3.1.5 Disaster Recovery Exercise Overview

3.1.6 Business Continuity

Table of Figures

Figure 2-1 Service Management: Service Support - Service Desk and Incident Management

Figure 2-2 Process for Post Go-Live Defects and Incidents

Figure 2-3 Red Alert and Crisis Indicators

Figure 2-4 Change Management Responsibilities

Figure 2-5 Release Management Concept Diagram

Figure 2-6 Release Management Overview

Figure 2-7 Release Management Release Cycle

Figure 2-8 Release Cycle Calendar

Figure 2-9 Configuration Management Standards

Figure 2-10 IT Asset Inventory Management Life Cycle

List of Tables

Table 2-1 Severity and Resolution Targets

Table 2-2 Valid Hold Criteria

Table 2-3 Production (ABEND) Response Guidelines

Table 2-4 SLAs

Table 2-5 High Risk Changes (C1-C2)

Table 2-6 Production Emergencies (CE)

Table 2-7 Risk Category C3 and C4

Chapter 1 Service Management Overview

Service Management is processes related to providing the operational products and services required to meet a Client's business needs. Service Management is divided into two major process groups, which are defined in the Information Systems (I/S) Rainbow Chart and I/S Management Practices Manual (MPM) as follows:

1. **Service Support** — Processes that allow Clients and Users to get access to the appropriate IT services to support their business. Clients are the persons authorized to conclude an agreement with the IT Organization about the provisions of IT Service and to ensure IT Services are paid for or the "pay the bill" people. Users are people in the Client Organization that use the IT Services for their routine activities or the "hands on the keyboard" people.
2. **Service Delivery** — Processes that ensure that the Client obtains the services needed to support their business. The services are a combination of availability and use of Production Systems in which IT and Client interact or participate simultaneously — the experience cannot be assessed in advance, but only when the service is provided.

1.1 Service Management Governance

Service Management is governed by several committees:

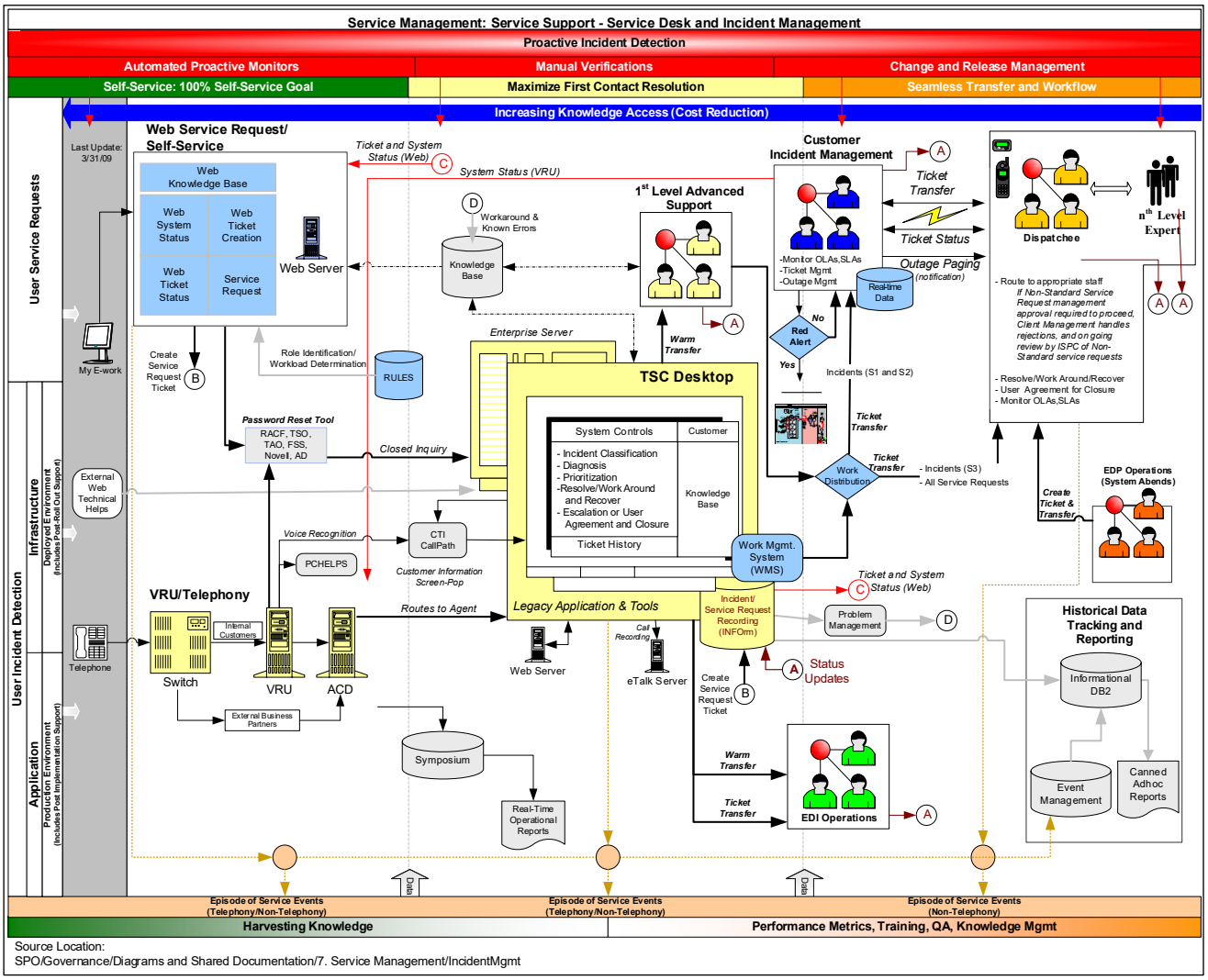
- **I/S Policy Committee**
  - The I/S Policy Committee (ISPC) and its standing subcommittees are responsible for the contents of the I/S MPM and provide management guidance to the I/S Standards Committee (ISSC).
- **ISPC Service Management Subcommittee**
  - Provides oversight for the policies and procedures for the Service Management Process (Break/Fix incidents and Service Requests).
  - Creates and/or updates policies to ensure an effective and efficient Service Management Process.
- **ISSC Incident/Problem Management Subcommittee**
  - Focuses on standards and workflow process changes related to Break/Fix incidents and Service Requests. Establishes and oversees the guidelines and standards that apply to the work done by I/S for Service Desk, Pro-Active System/Network Monitoring, Break/Fix, Critical Research, Service Request, and Problem Management.
- **ISSC Service Continuity Management Subcommittee**
  - Establishes and oversees the guidelines and standards that apply to the work done by I/S for Crisis Management and Disaster Recovery.
- **ISSC Capacity Management Subcommittee**
  - Establishes and oversees the guidelines and standards that apply to the work done by I/S for Service Level Management, Business Capacity Management, Service Capacity Management, Resource Capacity Management, and Availability Management and for optimizing applications and ICT infrastructure.

Chapter 2 Service Support

The section in this chapter provide details concerning the *Service Support* processes that allow the Information Systems (I/S) Division to focus on technical operations in support of running IT as a business inside a business.

2.1 Incident Management

This section contains standards and guidelines related to managing critical and non-critical issues or conditions to enable I/S to handle any issue that occurs in a timely and professional manner. BlueCross BlueShield of South Carolina (BlueCross) has adapted the Information Technology Infrastructure Library in defining its Incident Management processes. In the I/S Rainbow Chart, Incident Management is defined as "a reactive process with the goal of returning to a normal level of service, as defined in a Service Level Agreement. This is accomplished by the business activity of a Client Organization and its Users with the smallest possible impact." Currently, the processes for Incident Management apply to Break/Fix and Critical Research incidents and to Service Requests. This section is divided into Incidents (overall) followed by the specific standards for Break/Fix incidents and for Service Requests. The diagram (Figure 2-1) provided on the next page depicts the Incident Management process from the Management Practices Manual (MPM).



Source Location:
SPO/Governance/Diagrams and Shared Documentation/7. Service Management/IncidentMgmt

Figure 2-1 Service Management: Service Support - Service Desk and Incident Management

2.1.1 Incident Management Participation

All areas under the BlueCross Chief Information Officer participate in Incident Management and adhere to the Incident Management standards. Other non-corporate I/S groups may participate in Incident Management. The Incident Management standards include the following:

- Workloads are named WR-xxxx and SS-xxxx for Service Requests and Break/Fix incidents respectively.
- The Dispatch Model is used for Incident Management; this is the model where support area technicians receive work assignments from their Incident Management Dispatchers so that Incidents are managed and resolved in a timely manner.
- Tickets for Incident Management are worked from the Incident Management workloads, which are the formal record of the work.

2.1.2 Incidents

Per the I/S Rainbow Chart, incident processes are the "[p]rocesses related to the recording, monitoring, and closure of any event which is not part of the standard operation of a service, and which causes or may cause an interruption to or a reduction in the quality of that service."

The Technology Support Center (TSC) serves as the point of contact for Incidents. The I/S Service Management Support area is responsible for any official reporting for Incident Management.

2.1.2.1 Life Cycle for a Typical Incident or Service Request

Though there are slight variations due to some automation of how the Break/Fix incident or Service Request is reported, these are the typical steps in the life cycle:

- A customer reports the Break/Fix incident or Service Request, either by contacting the TSC or using a self-service method.
- The Break/Fix incident or Service Request is recorded and then referred to as the *ticket*.
- If the ticket cannot be resolved at first level, it is assigned to the appropriate area for resolution.
- The Dispatcher assigns the ticket to a Responsible Technician.
- The Responsible Technician resolves the incident or fulfills the requested service.
- The customer confirms the resolution.
- The Responsible Technician closes the ticket.

2.1.2.2 Recording a Break/Fix Incident or Service Request

The following are the approved sources for Break/Fix incidents or Service Request tickets:

- Telephone call to the TSC
- TSC Self-Service
- Enterprise Monitoring System
- Event Management

2.1.2.3 Incident Management Severity Level Definitions and Service Targets

Formal Service Level Agreements currently only exist between BlueCross and some of the external customers. However, Service Level Targets are in place to ensure the quick fulfillment of Service Requests and the resolution of Break/Fix incidents. The severity of the Break/Fix incident or Service Request is based on the impact to the business and is determined by criteria used by the Service Desk Specialist or the Incident Management Specialist. The expected time to resolve an Incident is referred to as *Resolution Target* and is monitored and overseen by the Incident Management Specialist. In the case of Service Requests generated by the TSC Self-Service, the default severity is determined when the form is added to the TSC Self-Service and is subsequently reviewed by the Service Desk Specialist or the Incident Management Specialist.

The table below (Table 2-1) describes the expectations regarding working the ticket to resolution and the criteria for determination of the severity, unless specific business contracts state otherwise. Resolution Targets listed are for original tickets. Assistance Requested and Approval Requested tickets are completed within operational level expectations, which allow the original ticket to be resolved within the Resolution Target. It is important to note the following:

- Only Incident Management tickets use the severity codes of S1, S2, S3, W1, W2 or W3.
- Incident Management records do not have other severity codes, except for Enterprise Monitoring Systems-generated informational tickets, which are created in a closed status and have the severity code of S9.
- System Support Groups have the option to prioritize within severity.

Severity and Resolution Targets

Severity & Resolution Target	Category	Criteria
S1 *85% of tickets completed within a Resolution Target of four hours* (worked by I/S 24x7, with customer contact availability 24x7)	Critical	Multiple* users experience a failure or interruption in the ability to perform a job function that has a significant impact to the business. Examples are listed below: • The Information Tracking System (INFOrm) is getting ABENDs. • Customer Service Representative (CSR) Desktop getting *page cannot be displayed* error. • AnyDoc Optical Character Recognition (OCR) getting *work not available* message. • Financial impacts, compliance/contractual impact or penalties. *A single-user *exception* can be made if it represents a significant impact to the business. The user must have a strong justification.

Severity and Resolution Targets

Severity & Resolution Target	Category	Criteria
S2 *85% of tickets completed within a Resolution Target of eight hours* (worked by I/S 24x7, with customer contact availability 24x7)	Urgent	Users experience a high impact problem where business is proceeding but cannot be completed in a normal manner. An acceptable work around may or may not be available and resolution is time sensitive. Examples are listed below: • Customer Care Manager (CCM) Desktop taking 30 seconds to display the end task screen. • TSC Desktop getting *page cannot be displayed* error. INFOrm is available. • Transaction XXXX is getting an ABEND but not every time and will process if tried again. • Screen clocking when the Enter key is pressed.
S3 *85% of tickets completed within a Resolution Target of 27 business hours* (worked by I/S Monday–Friday; 8:00 a.m.–5:00 p.m.)	Important	Users experience an issue that does not have significant business impact. Examples are listed below: • User is unable to receive a non-critical fax. • User workstation is not booting up, but they can work from another workstation. • Printer is making a funny noise. • User no longer has access to one of the two network printers in the area.
S9 *Monitoring tickets that are created as closed tickets if there is an entry in the Event Management Downtime Table*	Informational	When a monitor sends an alert to the Event Management system for processing, Event Management will create a ticket. If the application, server or service is in the Event Management Downtime Table, the ticket severity will be changed to an S9.

Severity and Resolution Targets

Severity & Resolution Target	Category	Criteria
W1 *85% of tickets completed within a Resolution Target of one business day* (worked by I/S Monday–Friday; 8:00 a.m.–5:00 p.m.)	Important	A business-critical request where urgent fulfillment is required, usually in no more than one working day. Some examples are: • Where there is a risk to security, data integrity or business productivity that needs urgent attention, such as an employee termination. • An external auditor is on-site needing access to an application.
W2 *85% of tickets completed within a Resolution Target of five business days* (worked by I/S Monday–Friday; 8:00 a.m.–5:00 p.m.)	Routine	A Service Request that should be filled within one work week. Most Service Requests are classified as W2. These are routine requests with medium impact to customer work activity or productivity, such as security requests or requests for packaged software installation.
W3 *85% of tickets completed within a Resolution Target of the customer agreed-upon date.* (worked by I/S Monday–Friday; 8:00 a.m.–5:00 p.m.)	Negotiated completion date	A Service Request where the completion date is negotiable or can be planned ahead with the requestor. This is for work that must be coordinated with the customer for a future-date deliverable, such as a workstation move. Another example would be a request to add a new set of users to an application system when a new company is added.

Table 2-1 Severity and Resolution Targets

2.1.2.4 Ownership

Incident Management bases the ownership of the incident or Service Request on the owner of the application, device or system that is experiencing the problem or needing service. This is regardless of severity or number of users impacted and may not necessarily be the area working the Incident.

For Incidents experienced through the use of an application, device or system, the Incident record is dispatched to the support area responsible for the application based on the Incident Ownership & Escalation Matrix (IOEM).

Transferring Tickets

Only the Support Specialist transfers Incidents from one owning support area to another and only when an error was made in the initial assignment. The Response Code of TECWA will denote this situation in the ticket. However, if the Incident scenario changes and the Incident ticket needs to be assigned to

another group, the Response Code of TECOC will denote the situation in the ticket. Incident Management Dispatchers may transfer Incidents between the workloads for which they are responsible. If there are ownership disputes, the Incident Management Specialist will make the final determination.

2.1.2.5 Resolving the Incident or Service Request

First In/First Out

Within each incident or Service Request Workload and within each Severity Code, the Incident Management Dispatcher and the Responsible Technician work the tickets on a first-in, first-out basis. Incidents may be prioritized within severity based on impact.

Requesting Severity Level Changes

After the Responsible Technician has reviewed and researched the Incident, the Incident may need to have a severity level change. The support area or Client Management may request the severity level change by contacting the Incident Management Specialist who will make the final determination.

Shared Responsibility of Resolution

If it is determined that the resolution requires assistance from another support area, the Incident Management Dispatcher/Responsible Technician requests assistance directly from the appropriate support areas. No changes are made in ownership. The Incident is not placed on hold while waiting for input from the other support area. The owner of the original ticket is responsible for completing all documentation, managing the timely resolution of the Incident, confirming with the customer when the Incident is resolved, and closing the ticket.

Estimated Completion Date and Time

The information entered in the Estimated Completion Date (ECD) date and time fields display on TSC Self-Service. The Responsible Technician and the Incident Management Dispatcher ensure that the ECD is updated as the status changes.

Any ECD change for W3 tickets must be coordinated with the customer.

Placing a Hold on a Ticket

There are times when the Responsible Technician will request to have the ticket placed on hold in keeping with the Hold Process described in the section *Hold Process* below. While the ticket is on Hold, the ticket is in a pending status. Reports will identify incidents that were placed on hold before resolution and closure.

Closure Process

- All Assistance Request and Approval Request tickets must be closed before the originating Incident ticket is closed.
- The Responsible Technician or Incident Management Dispatcher will confirm with the customer that the incident or Service Request is resolved and will update the incident or Service Request accordingly.
- If Computer Operations resolves a batch ABEND Incident, Computer Operations will close the incident.

Incident Details

After the Incident is resolved, the Responsible Technician enters information regarding the actual problem, the root cause and the steps taken to correct the Incident. This Incident Detail is required when an Incident is resolved (TECRI) or when closed (CL).

All Break/Fix incidents are documented with the completion of the Incident Detail prior to closure with the following exceptions:

- A batch ABEND Incident is being closed by I/S Operations.
- An Incident is closed within one of the workloads owned by the TSC.

Criteria for Re-Opening a Closed Incident

If a customer feels that their Incident was not resolved and the ticket was closed without their confirmation of resolution, the customer may request that the TSC re-open the ticket. The window for closure is based on severity and will affect whether the original Incident is re-opened or a new Incident recorded.

2.1.2.6 Hold Process

At times, an Incident may need to be placed on hold. The following valid hold criteria (Table 2-2) have been established for use on incidents and Service Requests. Incident Management Dispatchers must evaluate the ticket for valid hold criteria.

Valid Hold Criteria

Valid Hold Criteria

Scenario and Examples	Response Code	Verbiage to Display to Customer
Waiting for a batch cycle to run. • We have an incident that requires a two-part fix. The technician has made changes, but a batch cycle needs to run before the customer can actually verify that the issue is resolved.	HDBC	Waiting on a batch process to complete.
Code changes (non-Work Requests). • When changes to coding must be made to resolve an incident, that incident may be placed on hold while the code is changed and tested.	HDCC	Waiting on additional code changes.

Valid Hold Criteria

Scenario and Examples	Response Code	Verbiage to Display to Customer
Waiting on the customer. • When a customer is unavailable and there is no backup for the tech to contact for additional information or resolution verification. Information required must be documented in ticket. • When information or action is needed by the customer.	HDCI	Waiting on customer input.
The customer must ship or bring system in from a remote location. • At Home or cottage worker has a problem with equipment and it cannot be fixed via phone; therefore, they will need to bring the equipment on-site.	HDEC	Waiting on equipment from the customer.
Awaiting external/third-party vendor fix — vendor needed to correct issue. • A network printer needs a jack installed to connect. • An HP Deskjet printer cannot be repaired, or an IBM printer has malfunctioned and is still under warranty.	HDEX	Waiting on external vendor.
A customer requests a service to be performed at a future date. • The customer is contacted, and we are informed that it will be *x* days before the service can be performed.	HDFD	Waiting future date to begin work.
Parts on order. • Equipment cannot be repaired until software from an outside vendor has been received.	HDPO	Parts on order.

Valid Hold Criteria

Scenario and Examples	Response Code	Verbiage to Display to Customer
Waiting on a file transmission from an external customer. • Corrupt file is received. • Expected file is not received. • After research, it is determined that the problem resides on the customer side. • The customer is contacted, and we are informed it will be *x* hours before we receive the file. The number of hours could range from two (2) to 48+.	HDFT	Waiting on external data.
Purchase request is required. • The customer will need to submit a purchase requisition if additional software is needed but has not been purchased by the customer.	HDPR	Waiting on purchase requisition.
Software pushes. • When a software push is needed to resolve an incident, that incident may be placed on hold until a package is created and pushed to the customers.	HDSD	Waiting on software delivery.

Table 2-2 Valid Hold Criteria

Invalid Hold Criteria

Incident Management does not support the following reasons for placing a ticket on hold:

- Waiting on another area to complete their portion of work; though if the Assistance Required ticket is placed on hold for a valid reason, the original ticket may also be placed on hold.
- Waiting on activities to be completed by a project or change sheet.

When the Incident Management Specialist identifies that a ticket is on hold for an invalid reason, the Responsible Technician will be contacted and informed that the hold has been removed.

Requesting a Hold

For S1 and S2 tickets, the request for a hold is made through the Incident Management Specialist. For all other severities, the Responsible Technician adds the hold request response code to the ticket with documentation regarding the reason. The Responsible Technician will also validate the Estimated

Completion Date (ECD) date and time fields, ensuring that the ticket does not expire prior to the hold date. The Incident Management Dispatcher evaluates the hold request to determine whether or not to place the incident on hold. The Incident Management Dispatcher also evaluates the hold date requested against the ECD provided. The hold response code will display customer-friendly verbiage to the status sections of the TSC Self-Service.

Approving a Hold Request

Once the Incident Management Dispatcher validates the hold request, the Incident Management Dispatcher changes the status of the ticket to *hold* and then enters the expected expiration date and time of the hold, referred to as the Due Date, thus, approving the hold request. For S1 tickets, there must be an approval by the Director from the System Support Group and Service Management prior to putting the ticket on hold.

Denying a Hold Request

To deny a hold request, the Incident Management Dispatcher documents the ticket with the status update response code and adds comments indicating the denial of the hold request. The Incident Management Dispatcher then contacts the Responsible Technician to advise them of the hold denial and inform them to continue working on the ticket.

Hold Complete

The Incident Management Dispatcher monitors the ticket's Due Date so work can begin when appropriate. If the reason for the hold is satisfied, the Incident Management Dispatcher will update the ticket status to *open* and will reassign the ticket to the Responsible Technician. The Responsible Technician may also request for the hold to be released.

2.1.2.7 Oversight

Incident Management Administration

Application system administration for Incident Management is controlled by the TSC. This includes:

- Defining workload.
- Updating the Incident Ownership Matrix and Escalation Matrix.
- Updating code values for the Incident Management application systems.
- Managing user IDs for the Incident Management application systems.
- Updating the tools used for paging support areas and other I/S personnel.

Escalation Process

Incidents follow a defined Resolution Target time period based on the severity of the Incident refer to the Severity and Resolution Targets table above (Table 2-1).The Incident Management Specialist conducts escalation of Incidents based on the severity of the Incident and the length of time since the Incident ticket was created.

The Incident Management Specialist escalates the Incident through the appropriate chain listed on the Incident Ownership & Escalation Matrix until the Incident is resolved, and as appropriate for each severity.

Response Codes

Response Codes are vital to the Incident Management process. They document critical steps within the life cycle of an Incident.

2.1.3 Break/Fix Incidents

Per the I/S Rainbow Chart, Break/Fix processes are "related to the alteration or normal repair of a failure in the infrastructure or application systems. These processes include an escalation process based on operational system downtime or impact of failure."

Break/Fix incidents are defined as events that are not part of the standard operations of a service and that cause or may cause an interruption to or a reduction in the quality of that service.

2.1.3.1 24x7x365-Support

Because the Incident Management tickets with S1 and S2 severity codes require urgent attention, the responsible support organizations and impacted customers are required to provide on-call availability and contact information. The Incident Management Specialist will contact the on-call person by telephone to notify of the S1 or S2 ticket. Additionally, the Incident Management Specialist communicates the status of the S1 or S2 ticket via a paging process throughout the incident's life cycle.

2.1.3.2 Process for Post Go-Live Defects and Incidents

The Application Systems Management Framework describes how Break/Fix incidents are coordinated with Post Go-Live Defects for a Work Request.

Any defect reported during the Post Go-Live, Post Go-Live Support or Post Roll Out Support Phases that impacts Production software or operational infrastructure and has customer business operational impact (Figure 2-2) is also recorded in the Incident Management process as an incident by the I/S Test Designer. Any incident that may be attributed to the implementation should also be communicated to the I/S Test Designer to be recorded as a defect. It is the responsibility of I/S (e.g., the Work Request Team, the Systems Support and Operational Support areas) to ensure that both an incident and a defect are created to track the Production issue. I/S should err on the side of reporting incidents rather than not reporting them.

The incident ticket will remain open in the support area's workload until the customer impact is resolved. The record of the defect will assist the Work Request Team in tracking the issue and provide an historical record for future Work Requests for the affected application or infrastructure. The record of the incident will ensure timely resolution with the appropriate focus from the support areas and the Work Request Team as well as an historical record of the Production Post Go-Live Defect.

NOTE Before the Work Request can be closed, corresponding incidents related to the implementation should be resolved (closed) using the Incident Management process.

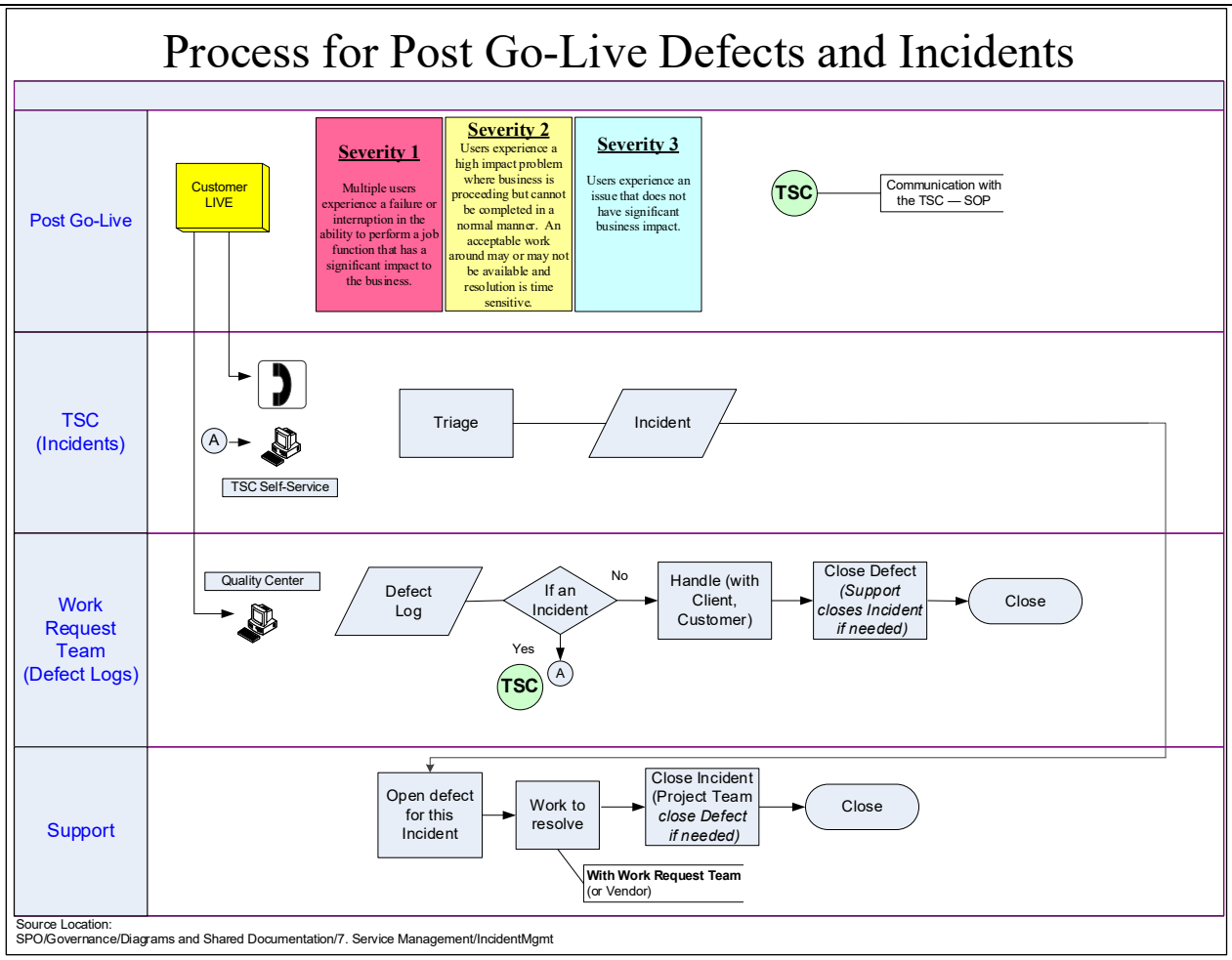


Figure 2-2 Process for Post Go-Live Defects and Incidents

2.1.3.3 ABENDs Detected

Computer Operations monitors the activity in the Data Centers. When there is an abnormal end (ABEND) of a process or Job running in the Data Center, the Computer Operator records a Break/Fix incident, using a user interface that enables automatic assignment of the incident to the appropriate Workload, paging of the on-call support staff and monitoring of all ABENDs. Computer Operations contacts the appropriate on-call personnel regarding the ABEND. The on-call personnel will typically be the Responsible Technician for that ABEND incident. Computer Operations records all ABENDs with the severity code of *S1*.

If requested, Computer Operations will serve as the Incident Management Dispatcher by assigning the incident to a specific Responsible Technician and updating the ticket record with the Responsible Technician's acceptance of the ticket.

If Computer Operations can resolve the incident, they will update the incident record and close it with the permission and instructions from the Responsible Technician. If Computer Operations cannot resolve it, the Responsible Technician will begin researching and documenting the incident record.

The Responsible Technician will use the appropriate response code *BATCH* to inform Computer Operations what action needs to be taken. This response code is used to document the incident record with progress, status, etc.

Production Problem (ABEND) Response Guidelines

Generally, any Production problem must be responded to immediately. In support of this objective, a Production-Crisis Level reporting scheme has been established. The purpose of this reporting scheme is to quickly identify the status of a given Production system so that I/S Management can ensure a proper response to a given problem.

The following (Table 2-3) defines the Production (ABEND) response guidelines used in the reporting scheme.

Production (ABEND) Response Guidelines

Level	Meaning	Action To Be Taken
0	Systems functioning normally	None
1	System Problem (ABEND) Occurs	Computer Operations contacts on-call/system support personnel.
2	System Problem is unresolved within two (2) hours.	Computer Operations notifies the on-call system support manager.
3	System Problem is unresolved within three (3) hours.	System Support management notifies the involved next level of management.
4	System Problem is unresolved within four (4) hours.	System Support management notifies the involved next level of management.
5	System Problem is unresolved within five (5) hours.	System Support management notifies the CIO and the TSC.

Table 2-3 Production (ABEND) Response Guidelines

It is the responsibility of the on-call personnel responding to a problem to periodically update Computer Operations with the level of each problem they are in the process of resolving. Based on the severity of the issue, it is left to the manager's discretion to accelerate the time line identified in the above guidelines. Even though the TSC must be notified when the Production crisis is at Level 5, the TSC should be notified at any point in the process when it becomes appropriate (depending on the problem).

2.1.3.4 Red Alert and Crisis Escalation Criteria

A Red Alert status brings an immediate level of attention to a critical incident, providing the framework for developing a rapid resolution. Service Management is responsible for identifying the required team members from the System Support areas and for facilitating efforts so that the team can focus to explore all possible solutions for resolution. In addition, the Red Alert process provides for clear, concise communication to the CIO and appropriate senior management.

Since the Red Alert process is an escalation of the Incident Management process, it follows all of the documented Incident Management processes.

If a Red Alert does not yield a timely resolution, or the criticality of the incident increases, the need to declare a Crisis may be necessary. The Red Alert process includes consistent and timely reviews during the Red Alert activities to determine if a recommendation to engage the Crisis Management team is warranted.

Declaration of a Red Alert

Information for triggering a Red Alert is derived from several factors including, but not limited to:

- A lack of clear identification of what the actual problem is.
- No clear owner has been established.
- No progress is being made towards resolution.

The time frame for reviewing whether an incident meets Red Alert criteria is based on Severity, as follows:

- S1 During the first hour of ticket open
- S2 During the first two hours of ticket open
- S3 Four (4) business days from ticket open

If a Red Alert is not declared, the criteria will be reviewed during the time frame for an Incident Management status update, again, based on Severity:

- S1 Every hour
- S2 Every two (2) hours
- S3 Every one (1) business day

Recommendation for a Crisis

A recommendation that a Crisis should be declared will be determined by a consensus of Service Management, the respective System Support area, Application Owner and Direct Report to the CIO.

The time frame for reviewing whether a Red Alert should become a Crisis recommendation is the same for all severities: two (2) days from the declaration of the Red Alert.

If a Crisis recommendation is not warranted, the criteria will be reviewed at the end of each day during the Red Alert.

The diagram below (Figure 2-3) depicts the relationship between the Incident Management resolution, Red Alert and Crisis Management.

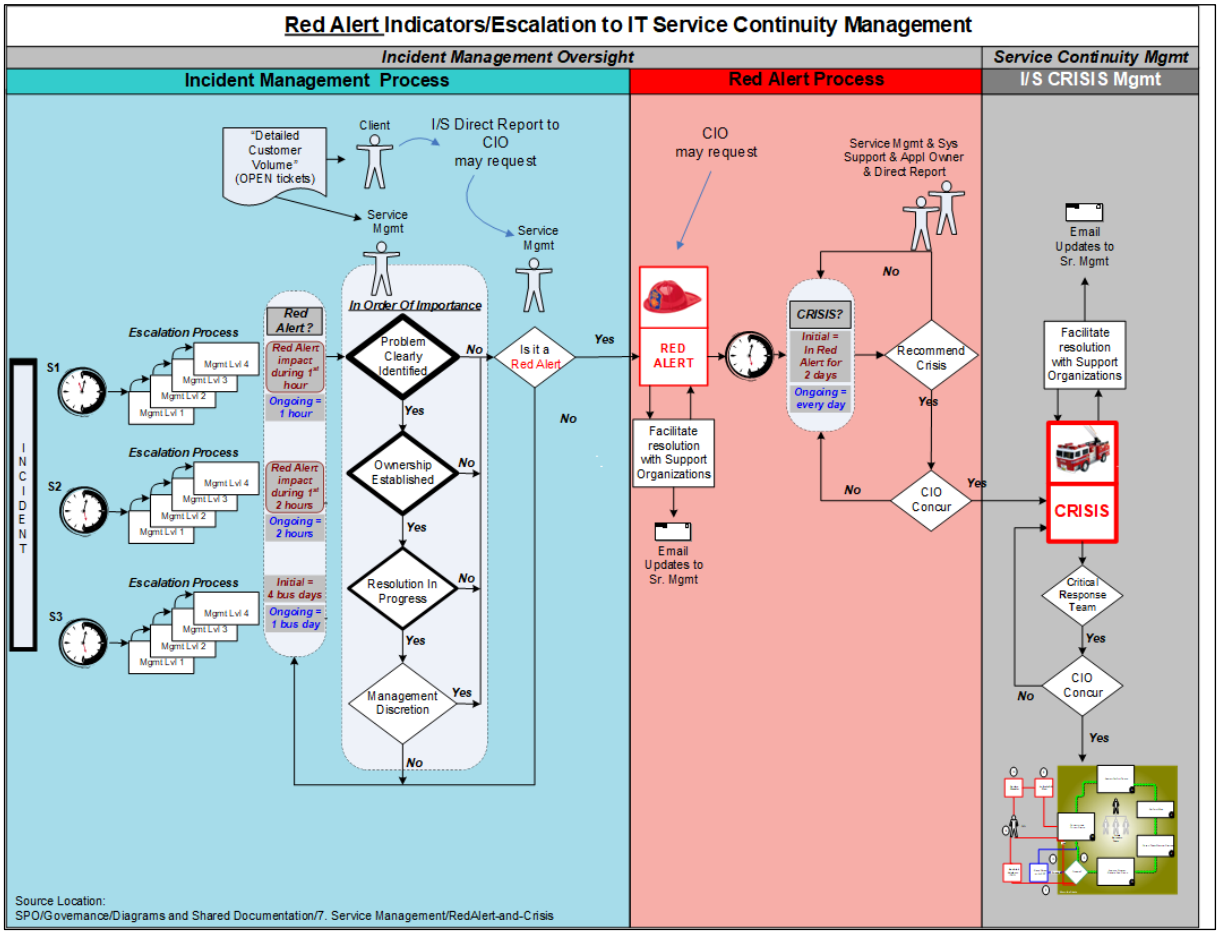


Figure 2-3 Red Alert and Crisis Indicators

2.1.4 Emergency Changes

Emergency changes are required to prevent or repair processing errors in Production that will severely inhibit the customers' ability to conduct their business. Application managers are responsible for ensuring that the proper level of support is available for their systems and that those persons who provide that support are fully briefed on the process for applying emergency fixes to Production.

An Emergency Change is an urgent request due to a Production issue or data corruption that jeopardizes the integrity of the system, prohibits the Production cycle from continuing, or has severe external exposure, and there is no other option. Incident tickets are created and assigned to the appropriate I/S area. The severity of the incident is dictated by its impact to the user community. The severity assigned to the incident determines the applicable Service Level Agreement (SLA).

While an Emergency Change is the result of an S1 severity incident, not all S1 severity incidents qualify as Emergency Changes. Whether an incident is to be handled as an Emergency Change or not is at the discretion of the I/S Manager assigned the responsibility for the incident.

The general rules for an Emergency Change are:

1. The Emergency Change can only address the issue defined by the problem affecting Production processing or data.
2. The Emergency Change must follow all Change Management documentation and approval procedures.

The I/S Manager will engage other departments or teams to resolve the issue within the agreed upon SLA. All work performed as a result of the ticket must be documented.

2.1.5 Critical Research

Per the I/S Rainbow Chart, Critical Research processes "respond to day-to-day Production System Incidents that involve requests for detailed technical research from the Applications Systems or Infrastructure areas, and result in the identification of manual workarounds, or the execution of a Break/Fix process."

2.1.6 Service Request

The I/S Rainbow Chart states that Service Request processes are "related to the fulfillment of requests from a User for support, delivery, information, advice, or documentation as defined as a 'standard service' under an SLA[,] which is not related to a failure in the infrastructure or would result in the alteration of the application or infrastructure."

2.1.6.1 Definition of a Service Request

A Service Request is a request for routine work to be completed by Information Systems (I/S) that is tracked and monitored, reported on and measured.

Service Requests are one of the core units of work that I/S performs. They are managed as part of the Incident Management process. The TSC and Incident Management Specialists provide operational oversight for the completion of Service Requests.

2.1.6.2 Service Request Process

Submitting a Service Request

A Service Request is made by notifying the TSC via a telephone or submitting a Service Request form using the TSC Self-Service on My e-Work. A Service Request can also be made using those methods by a third party on behalf of the requestor, such as a Client Advocate after a discussion with a customer.

Recording of Service Requests

The Incident Management Process records information about the requestor, the request being made and the subsequent updates about how the request is fulfilled. Each I/S department or area that fulfills Service Requests has its own workload lists within the Incident Management (IM) Process to manage the requests. The Service Requests are classified by the severity codes listed in the Severity and Resolution Targets table. Refer to Table 2-1 in the section *Incident Management Severity Level Definitions and Service Targets* above.

Service Request Forms Review

As necessary, the ISPC Service Management Subcommittee will initiate a review of the list of Service Request forms. The Service Management area will provide usage information for each Service Request form. The ISSC Incident/Problem Management Subcommittee will review the data and make recommendations to the ISPC Service Management Subcommittee. Based on this evaluation, the Service Request form will either be continued, or it will be eliminated by submitting the Service Request titled *Service Request Forms - Delete the Form*.

Service Request Forms Development and Maintenance

NOTE The *Form Owner* or *Fulfiller* is the manager of the area that fulfills (works) the Service Request.

Process Audit oversees the addition, changing or deletion of Service Request forms and creates the appropriate Assistance Required tickets to engage the teams supporting the Service Request forms process.

For any complex forms requiring business logic within the form, the Form Owner should work with their Client Manager to submit a Work Request. I/S fulfilled-forms that are complex will require justification and a Work Request.

Adding a New Service Request Form

If a Fulfiller requests a new Service Request form in order to provide a routine service, the Form Owner will submit the Service Request titled *Service Request Forms - Add New Form*. Process Audit will present the request to the ISPC Service Management Subcommittee for review. If approved, the subcommittee will present the request to the ISPC for its approval and recommend that I/S should provide the service.

Changing an Existing Service Request Form

The Form Owner or designated representative may request changes to an existing Service Request form by using the Service Request titled *Service Request Forms - Change A Form*.

Deleting an Existing Service Request Form

The Form Owner may request the deletion of a Service Request form by submitting the Service Request titled *Service Request Forms - Delete the Form*. Process Audit will update the Service Request Catalog.

2.1.7 Contacting a Vendor about a Problem

Before opening a problem ticket with a software or hardware vendor, at least one of the following roles listed in the System Master Index must be consulted to confirm the action: Architect, Technology Owner or Vendor Relationship Owner.

2.2 Problem Management

2.2.1 Overview

Problem Management (PM) is a process in which activity and information (output) from the Incident Management processes are analyzed in search of reoccurring or otherwise significant problems and appropriate parties are engaged to understand the problem (Root Cause) and develop an appropriate response (Solution Design). The output of the PM process is a record of the problems, with their Root Causes and Solution Designs documented, in the known error database (PM Database [PMDB]), which is available to contributing entities in the I/S organization. Incident Management, application owners, and other interested parties use the PMDB and its output to prevent incidents and reduce the impact of future Incidents and improve processes and systems to reduce the opportunity for error.

2.2.1.1 Problem Management Purpose

In the context of the PM process at BlueCross BlueShield of South Carolina (BlueCross), a Problem is an abstract, high-level consideration of one or more incidents or events. The concept of the Problem includes the Root Causes, impacts, and workarounds of the issue. PM's role is to identify problems through trending and work with other teams to investigate, record the problem, and decide on and document appropriate measures to resolve or reduce impact. Trending includes analysis of Incident Details Screen (IDT), Customer Health, Post Maintenance Window, and Abends data as well as reviewing the daily Noteworthy report and analyzing the documented impact to the user community. PM will also consider adhoc trending when requested.

2.2.1.2 Problem Initiation and Owner Engagement

Once the Problem Record is opened and all known information is entered, the PMDB generates and distributes an initial request email, which includes deliverables for Root Cause and Solution Design, to the Problem Owner. The Problem Owner is to then complete a PM Questionnaire using a link provided in the email to log into the BOIT system. Once the questionnaire is completed and saved, a notification is sent to the PM Analyst who will review the response and discuss any outstanding questions as appropriate. The PM Analyst also needs to consider the following points regarding the meeting:

- In the invitation, the PM Analyst should include any questions that will be covered during the call so that the Problem Owner has time to prepare in advance.
- Whenever possible, the PM team should attempt to schedule a joint meeting between the PM Analysts and the Problem Owner so that all outstanding Problems may be discussed in a single call.
- The PM Analyst will send a meeting recap to the Problem Owner documenting any outstanding questions and define an Estimated Completion Date (ECD) for the response to those questions.
- If the Problem Owner does not join the call/meeting, the PM Analyst should send an escalation email to the Problem Owner and their manager for assistance.

Upon completion, the PM Analyst will send the Problem Owner a request to perform an accuracy review of the Problem Closure Document to ensure that the information is accurate and complete prior to moving to the next phase of the PM process.

2.2.2 Roles and Responsibilities

2.2.2.1 Problem Owner

The normal process is to assign a Problem Record to the manager of the support area that resolved the most significant incident in the record to-date; however, when there is no external customer impact and the support area itself is the impacted party, the Problem Record may be assigned to the manager of the application development area or manager associated with the System Master Index (SMI) item. The problem should not be reassigned later unless the original assignment was truly inaccurate, or the organizational structure of the assigned manager has changed.

Problem Owner's Responsibilities:

- Provides Problem Management (PM) with responses when requested and does so within the SLA or timeline established with the PM Analyst (Table 2-4).
- Works with all teams to gather needed information on Root Cause, Immediate Actions, and Solution Design.
    - Root Cause and Solution Design should be provided prior to the due date so any follow-up questions can be addressed.
    - If the due date is not achievable, the PO/Designee is to work with the PM Analyst to define a date acceptable to both parties.
- Assists in defining additional deliverables that might be needed due to additional research of the issue.
- Reviews the Postmortem document for completeness and accuracy.

SLAs

Priority	Impact	Root Cause SLA	Solution Design SLA	Accuracy Review SLA
P1	Extreme & Widespread	2 Business Days	5 Business Days	1 Business Day
P2	Critical or Severe	5 Business Days	10 Business Days	1 Business Day

Table 2-4 SLAs

2.2.2.2 Problem Management Analyst

This is the analyst assigned to manage the Problem Record. This PM Analyst is responsible for:

- Following up on deliverables and other updates required to fulfill the Problem Record.
    - This also includes updating the Problem Record log with any communications or information provided. The log is to be maintained daily.

- Reviewing their Problem Records daily for outstanding requests or deliverables that are due that day.

The Responsible, Accountable, Consulted, Informed (RACI) Chart below outlines the participation of various roles relative to PM (Table 2-5).

RACI Chart

Task	PM Manager	PM Analyst	Problem Owner	Tech Staff	Client
Problem Identification	A	R	C	C	I
Root Cause and Solution	C/I	C/I	A	R/C	I
Coordinate between Various Support Teams	I	R	R/A		C/I
Raising RFCs to Resolve Problems	I	I	R/A	R	C/I
Single Point of Contact for Assigned Problems			A		
Life Cycle of the Problem	A	R	I	I	I

- R — Responsible: The people who are responsible for correct execution — for getting the job done.
- A — Accountable: The person who has ownership of quality and the end result. **Only one person can be accountable for each task.**
- C — Consulted: The people who are consulted and whose opinions are sought. They have involvement through input of knowledge and information.
- I — Informed: The people who are kept up to date on progress. They receive information about process execution and quality.

Table 2-5 RACI Chart

2.2.3 Problem Escalation

Three levels of problem escalation have been identified and documented. If during the process, the Problem Owner does not respond to a request within one (1) business day after the established SLA, the PM Analyst is to initiate the PM escalation procedure. The initiation of the escalation procedure is at the discretion of the PM Analyst as there may be extenuating circumstances that impact the Problem Owner's ability to meet the SLA.

The procedure is as follows:

- **Phase 1 — 1 business day with no response after SLA**

- A communication (email and phone call) will be issued to the owner of the deliverable requesting the sought-after information to be provided. Both the Problem Owner's manager and the PM Manager will be copied on the email correspondence for awareness.

- **Phase 2 — 1 business day after Phase 1 with no response**
  - A communication (email) will be issued to the manager of the Problem Owner of the deliverable. The Problem Owner and PM Manager will be copied for awareness.

- **Phase 3 — 1 business day after Phase 2 with no response**
  - An escalation will be sent to the PM Manager to engage Senior Management.

2.3 Change Management

2.3.1 Purpose

The Change Management System ensures that all alterations to infrastructure hardware and software (both System and Network), and environmental facilities are approved by management and scheduled in advance. Change Management provides a consistent, quality of change implementation and reduces the number of changes that have to be backed out. Standardized methods and procedures are used in change categorization, development, testing, and implementation of all data processing changes, which provides accurate and timely change-related information that supports management decision-making regarding processing changes.

2.3.2 Change Flow

The general flow of a change through the Change Management process is outlined in Figure 2-4 on the next page. The process begins with the entry of a change request containing the proposed change into the INFOrm database via the Infrastructure Modification Approval Process (IMAP). INFOrm communicates the proposal between the various departments involved. The departments evaluate the technical feasibility, potential risk, and the effect of installing the proposed change in the production environment. The results and recommendations of this technical assessment are reported to management. A business assessment of the proposed change is performed that considers such items as monthly cutoffs, customer workloads, and current problems.

The recommendations from both the technical and business assessments are reviewed to determine if a change should be installed, delayed, or rejected. These decisions result in a prioritized installation schedule for approved changes. IMAP tracks the installation schedule using the Estimated Completion Date (ECD). IMAP requires the ECD so Release Management may communicate imminent and future implementations in the production environment to the organization. Refer to the section *Release Management* below for further details.

Validation of a change is performed and documented. The results of validation are entered into the Request for Change (RFC) ticket and communicated to all parties concerned including the Responsible Technician or Team Lead of the support area. The results are reviewed operationally by the I/S Change Management Office (CMO) by validating appropriate testing codes on the RFC.

For changes that cannot be validated prior to production implementation, the RFC will include verbiage identifying what could not be validated, along with a particular Change Management code indicating that the change meets pre-defined criteria for changes that cannot be validated. The Change Management code and specific reason for not testing a change will become part of the Change Implementation review/approval process.

NOTE Use of the particular Change Management code is defined in the CMO procedures.

The pre-defined criteria are documented within each departmental desk procedure.

The Change Submitter and Service Management Analyst ensure that all other related changes are either installed or scheduled for installation. The installation of a change is monitored, documented, and the results are communicated to all parties concerned. Management periodically reviews the effectiveness and efficiency of the Change Management processes by evaluating various informational reports and examining change-related failures as well as successes to see if they produced expected results. Risk-related categories are reviewed.

Assessment by management of planned and emergency changes affecting the production schedule shall occur on an as-needed basis in all technical areas prior to the I/S Weekly Scheduling Meeting. Change Assessment Management is the responsibility of the implementing department's management prior to the I/S Weekly Scheduling Meeting.

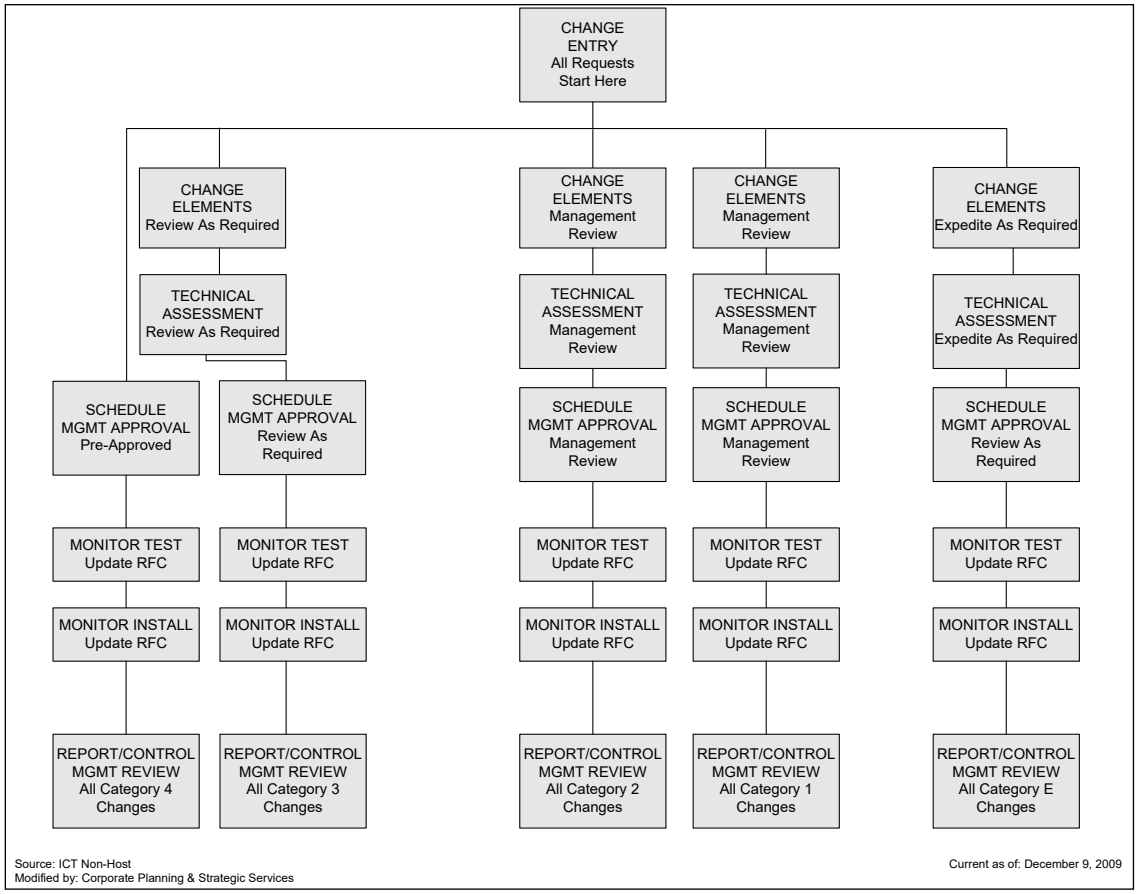


Figure 2-4 Change Management Responsibilities

2.3.3 Change Management Meetings

- The **Weekly Change Advisory Board (CAB) Meeting** is a cross functional group set up to evaluate new requests for technical need, priority, cost/benefit, and potential impacts to systems or processes. The CAB makes recommendations to proceed with the effort, further analysis, deferment, or cancellation.
- A **Weekly Quality Assurance (QA) Meeting** is conducted by area-submitting departments.

  - The Weekly QA Meeting is held by area-submitting departments prior to the Weekly CAB Meeting.
  - The Weekly QA Meeting is used to review change implementation from a technical and business point of view and to discuss the potential impact on the system and its users.

- During the I/S **Weekly Scheduling Meeting**, the Change Management Meeting Report is used to obtain management approval for change scheduling, review and confirm the change schedule, and to resolve any scheduling conflicts. Approval is validated during the meeting.

  - The Service Management Analyst produces the Change Management Meeting Report containing the changes scheduled for the upcoming weekend. The statuses of all scheduled changes are reviewed, and any action plans, issues, and concerns are discussed during this meeting.
  - As a result of these meetings, the Change Management Meeting Report is updated and distributed. Any changes not submitted and approved by the deadline of 3:59 p.m. following the day of the I/S Weekly Scheduling Meeting are cancelled by the CMO.

- The **Weekly Post Change Cycle Results Review** is used to review and confirm the results of the changes, which occurred during the previous Change Cycle (Monday through Sunday).

  - The Service Management Analyst produces the Weekly Results Report containing results information related to the previous change cycle changes. The results of all changes are reviewed. Any action plans, issues, and concerns are discussed with Information Communication Technology (ICT) Management.

2.3.4 Management Procedures and Responsibilities

2.3.4.1 Change Entry Procedures

The submission of a production change is accomplished by entering the change information directly via a **Request for Change (RFC)**:

- It is the responsibility of the **Change Requestor** to obtain approval from their manager prior to entering the change request.
- The **Technical Area Manager** responsible for implementing the change then must risk categorize the change according to the following listing and to supply any supporting documentation to the Service Management Analyst.

Risk Categories C1, C2, C3, C4 and CE must be approved as follows:

- **RISK CATEGORY 1 (C1)**

  - The change has the potential of having a major impact on a system or users, has high visibility, requires a long period of time to install, and/or will be difficult or impossible to back out.
  - The minimum lead time for this change is normally 21 days or one (1) day in emergency situations.

- **RISK CATEGORY 2 (C2)**

- The change may have significant impact, high visibility to multiple users, and/or will require involved back-out procedures.
- The minimum lead time for this change is normally 14 days or one (1) day in emergency situations.

- **RISK CATEGORY 3 (C3)**

  - The change has low visibility and is easily backed out.
  - The minimum lead time for this change is normally seven (7) days or the same day if an emergency situation.

- **RISK CATEGORY 4 (C4)**

  - The change has minimal impact (routine changes).
  - The minimum lead time for this change is normally four (4) days or the same day if an emergency situation.
  - For C3 and C4, service list items are pre-approved by area management.

- **RISK CATEGORY E (CE)**

  - This is an emergency change and must be approved by senior management.
  - The purpose is to have the emergency assessed as to impact and to notify affected customers.

The Technical Area Manager (or management designee) responsible for implementing the change must approve the request prior to implementation.

High Risk Changes (C1-C2) must have the following approval (Table 2-5):

High Risk Changes (C1-C2)

Implementing Area (C1-C2)	Approver
Host Software	Director, Technical Support or Management Designee
Non-Host Software	Director, ICT Non-Host or Management Designee
Database	Director, Database Administration or Management Designee
Network and Related Hardware	Director, ICT Non-Host or Management Designee
CDS Voice & Data Communication changes performed in Dallas	Director, CDS Client Voice and Data Communications or Management Designee
All Other	Director, Information Systems Operations or Management Designee

Table 2-5 High Risk Changes (C1-C2)

Production Emergencies (CE) must have the following Approval (Table 2-6):

Production Emergencies (CE)

Implementing Area (CE)	Approver
Host Software	Vice-President, Technical Support or Management Designee
Non-Host Software	Vice-President, ICT Non-Host or Management Designee
Database	Vice-President, Database Administration or Management Designee
ICT Network and Related Hardware	Vice-President, ICT Non-Host or Management Designee
CDS Voice & Data Communication changes performed in Dallas	Vice-President, CDS or Management Designee
All Other	Vice-President, Information Systems Operations or Management Designee

Table 2-6 Production Emergencies (CE)

The Service Management Analyst verifies that the request is entered into the INFOrm database.

2.3.4.2 Change Assessment

This technical/business assessment is performed, by area management, to make the following determinations regarding the requested change:

- To appraise the technical risk and potential impact the change may have during and immediately following implementation.
- To provide recommendations to management concerning the changes before they are implemented.

2.3.4.3 Security Assessment

Information Communication Technology (ICT) will perform a security assessment to determine any potential security/privacy/availability impacts resulting from the infrastructure change. The impacts will be logged to the RFC, as outlined in the Change Management Office (CMO) procedures. The CMO procedures will be available and provided to all ICT stakeholders, along with the appropriate System Security Officers for process engagement, review and feedback as described in the CMO procedures.

2.3.4.4 Change Implementation

Changes are scheduled during the I/S Weekly Scheduling Meeting. The Service Management Analyst may escalate the implementation of changes based on technical and/or business reasons.

The following (or management designee) must approve the production change and implementation schedule for categories C1–C4 and CE:

- Change Manager, Change Management or designee
- Area Manager of Requested Change or equivalent-level designee
- Director, ICT Non-Host or equivalent-level designee
- Director, ICT Host/Technical Support or equivalent-level designee
- Director, Information Systems Operations or equivalent-level designee
- Director, CDS Voice and Data Communications or equivalent-level designee (for CDS changes performed in Dallas)

In addition, for Emergency (CE) production change testing and implementation, the following must also approve for their area's requests:

- Vice-President, ICT Non-Host or equivalent-level designee
- Vice-President, ICT Host/Technical Support or equivalent-level designee
- Vice-President, Information Systems Operations or equivalent-level designee
- Vice-President, CDS or equivalent-level designee

The ICT area performing the infrastructure change will follow their respective guidelines and/or system documentation for the validation of the infrastructure change. Infrastructure changes are communicated to I/S Application, Project and Client organizations prior to implementation. They will assess the changes and may arrange for validation. Any validation and the communication of issues will follow agreed-upon plans, processes and/or procedures for their respective areas.

The ICT areas will note on the infrastructure Request for Change (RFC) testing results using the response codes as outlined in the Change Management procedures.

NOTE Changes related to Production Break-Fix tickets follow Incident Management policies and procedures.

NOTE Several infrastructure configuration changes are associated with highly repeatable processes and present minimal risk and impact to the infrastructure. The following requests (Table 2-7) categorized as Risk Category C3 and C4 are not required for scheduling during the I/S Weekly Scheduling Meeting.

Risk Category C3 and C4

Configuration Change	Configuration Category Code	Description
Firewall	FWREQ	Request to implement, update, or remove a Firewall Rule
Big IP Pool Updates	BIGUPDT	Update/Changes to existing IP Pools

Risk Category C3 and C4

Configuration Change	Configuration Category Code	Description
MQ Configuration Changes	MQCONFIG	Update/Change to MQ Configuration
Dynamic Host Configuration Protocol (DHCP) Changes	DHCPCG	Update/Changes to existing DHCP services
Virtual LAN	VLAN	Network Group-Switched Network
Virtual Private Network Update	VPNUPD	Update/Change to existing VPN Address
Secure File Transfer Protocol (FTP)	SFTP	Secure FTP Account Changes

Table 2-7 Risk Category C3 and C4

2.3.5 Service Management Analyst Responsibilities

The Service Management Analyst is responsible for ensuring that changes are entered into the INFOrm database, scheduling Change Management System meetings, and reporting results of these meetings to appropriate management. The Service Management Analyst is also responsible for the daily operation of the Change Management System and the integrity of the change data in the INFOrm database.

Responsibilities of the Service Management Analyst include, but are not limited to, the following:

- Conduct/Co-Chair the **I/S Weekly Scheduling Meeting**.
- Act as the focal point by communicating with all individuals, groups, and management regarding changes.
- Oversee the daily operation of the Change Management process.
- Report the results of technical/business assessment to management.
- Provide appropriate change reports and production schedules to the attendees of the **I/S Weekly Scheduling Meeting**.
- Notify users, the change requestor, and all other affected parties when a change is to be installed. The vehicle for this is the **Weekly Change Schedule**.

When a change is implemented in production and fails, the Service Management Analyst notifies the respective area's Senior Manager for management action. The vehicle for this is the **Weekly Change Results Report**.

When a change is implemented in the production environment that successfully resolves a problem recorded in the Infrastructure Modification Approval Process System, the Service Management Analyst is notified, and the problem is closed. The vehicle for this is the **Weekly Change Results Report**.

The Service Management Analyst produces a monthly status report showing:

- The number of changes logged.
- The number of changes completed.
- The total number of outstanding changes remaining.

- The distribution of changes by category and type.

System availability statistics are reported by Incident Management Support monthly.

2.3.6 Change Management System

The purpose of the Change Management System is to ensure that standardized methods and procedures are used in change development, validation, and implementation. To achieve this goal, the procedures documented in the Configuration Management Plan manual must be followed (Refer to the *Service Management* Volume of the ISSM for details.). This process is known as IMAP.

2.3.6.1 Hardware/Software Standards

Non-Host infrastructure standards include all hardware and software technologies approved for use in the Non-Host environment.

The standards contained in *Security Management* > *Information Security Management* provide:

- High-level descriptions regarding ICT NH technologies.
- The products and systems within each technology.
- The approved use for those products within the company.
- Any approved exceptions to those standards.

Technical Standards contain:

- Approved product versions.
- Detailed standards for deployment and operations.
- BlueCross BlueShield of South Carolina best practices.

2.4 Release Management

2.4.1 Release Management Introduction

As IT industry best-practice frameworks have become available, the Information Systems Division adopted a philosophy of reviewing and selectively adapting components from these frameworks to its internal needs.

As part of these best practices I/S chose to adapt aspects of the Information Technology Infrastructure Library (ITIL), the Capability Maturity Model Integration (CMMI) Control Objectives for Information and related Technology (COBIT) and the Enterprise Architecture Maturity Model (EAMM) for their foundation.

In adapting Release Management best practices, I/S took a holistic (people, process, technology) view, which considers all aspects of a change including planning, authorizing, monitoring and analysis. For a graphic representation of Release Management, please see the concept diagram below (Figure 2-5).

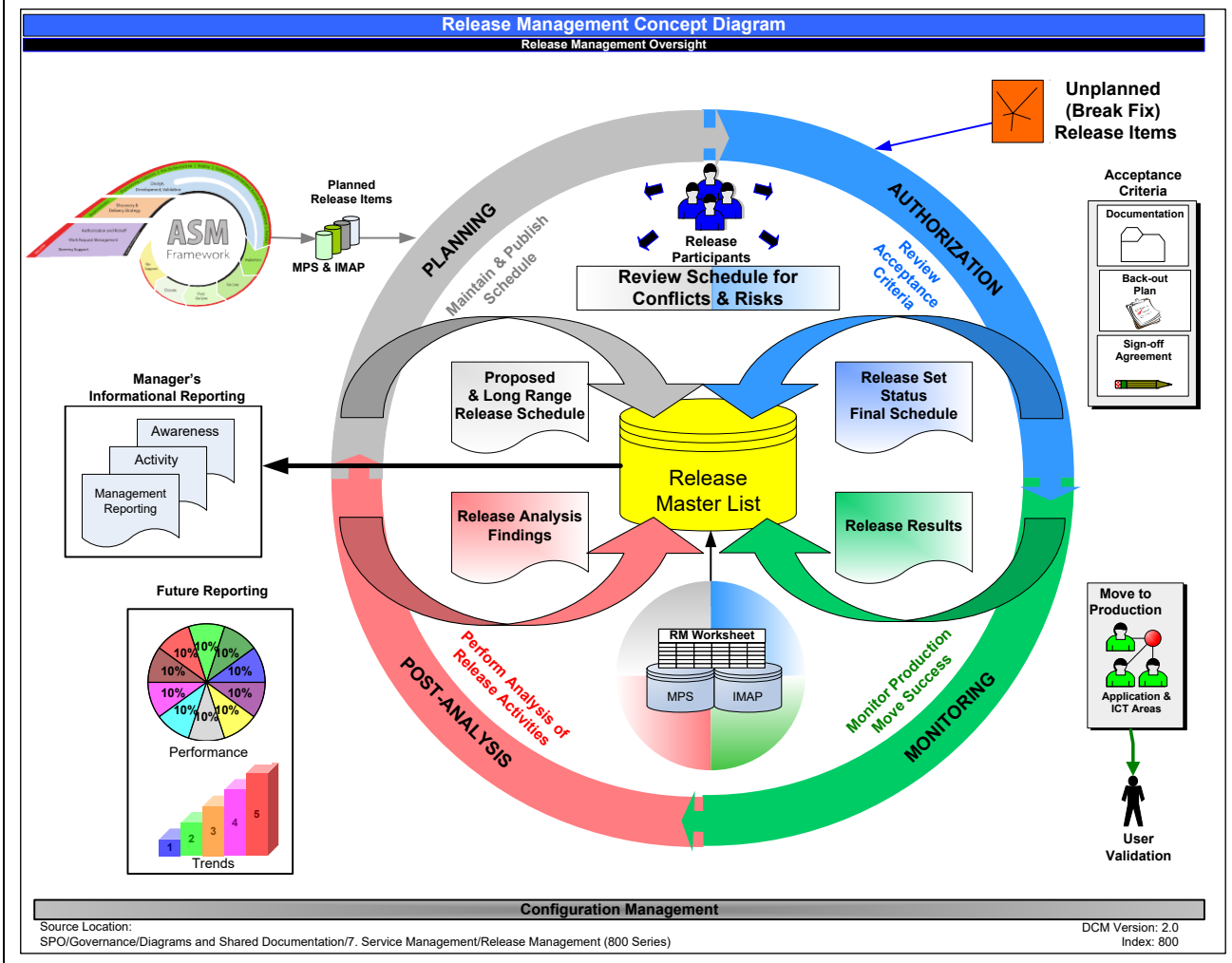


Figure 2-5 Release Management Concept Diagram

Release Management will benefit I/S by providing a vehicle for better communication of changes and higher quality implementations.

The communications are better because of the following:

- Published Release Schedules
- Weekly meetings discussing the current release schedule
- Monthly meetings discussing long range release planning
- Comprehensive analytic and performance reporting
- Dedicated Release Management Office, who facilitates the RM process

NOTE The #1 Objective for Release Management is Successful Communication.

The quality of implementations improve through

- Release Master List storing historical and future release information.
- Enhanced focus on planning activities.
- Additional support of System Support and SEM acknowledgements.
- Documentation of items released into production.
- Post -Analysis reporting for review and trending of performance.
- Standard release management processes comprised of industry best practices.

In Figure 2-6 on the next page, we see how the I/S department adapted various phases of Release Management.

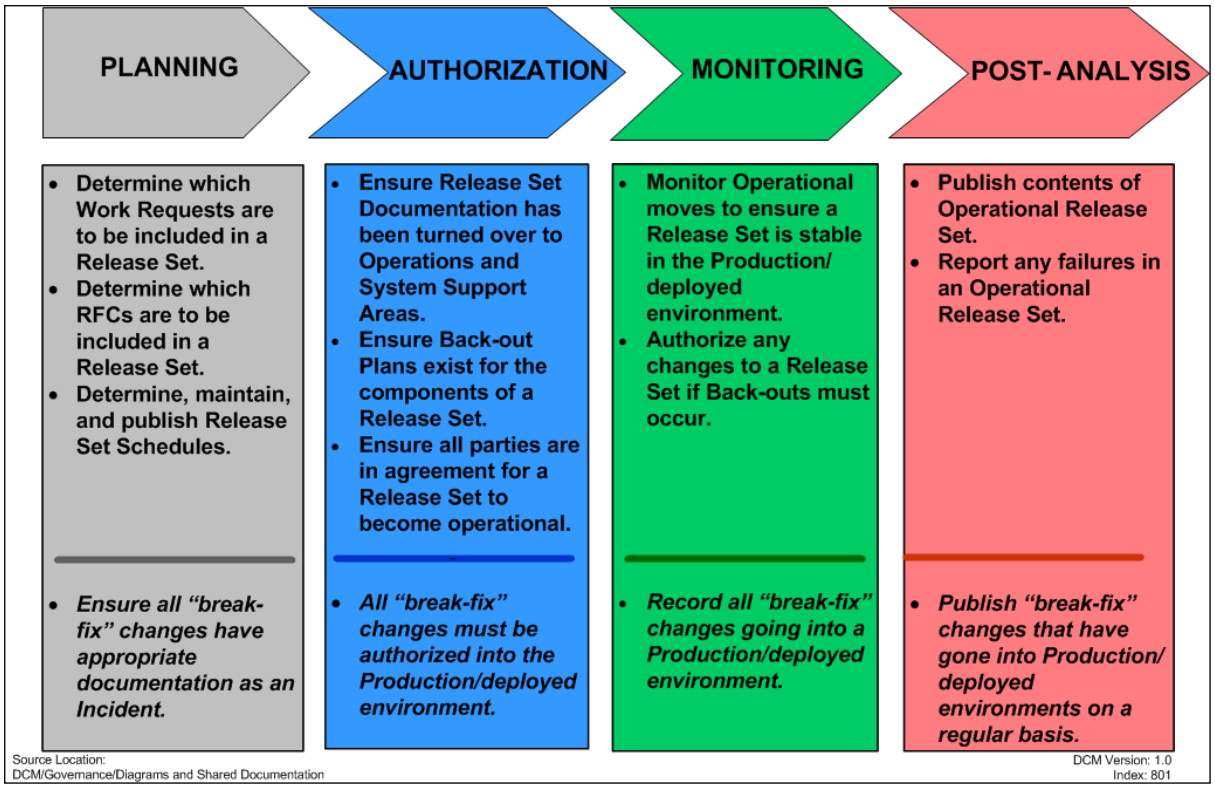


Figure 2-6 Release Management Overview

Release Management is overseen by the Service Management Sub Committee of the I/S Policy Committee. Before any changes are made to the processes, the changes must be reviewed and approved by this subcommittee and the I/S Governor.

2.4.2 Release Management Process Overview

As stated before, the Release Management processes for the I/S Division of BlueCross BlueShield of South Carolina (BlueCross) consists of four unique phases that make up a Release Cycle — Planning, Authorizing, Monitoring and Post-Analysis. Planning communicates what we ***want*** to do, Authorizing communicates what we ***will*** do, Monitoring communicates what we ***did*** and Post Analysis communicates ***how well*** we did.

A Release Cycle occurs each calendar week consisting of all the items implemented into a Production/deployed environment during that time frame. Below is a context diagram (Figure 2-7) that shows each phase of the release cycle and how they are related. A more in-depth explanation of each phase will be provided later in this section.

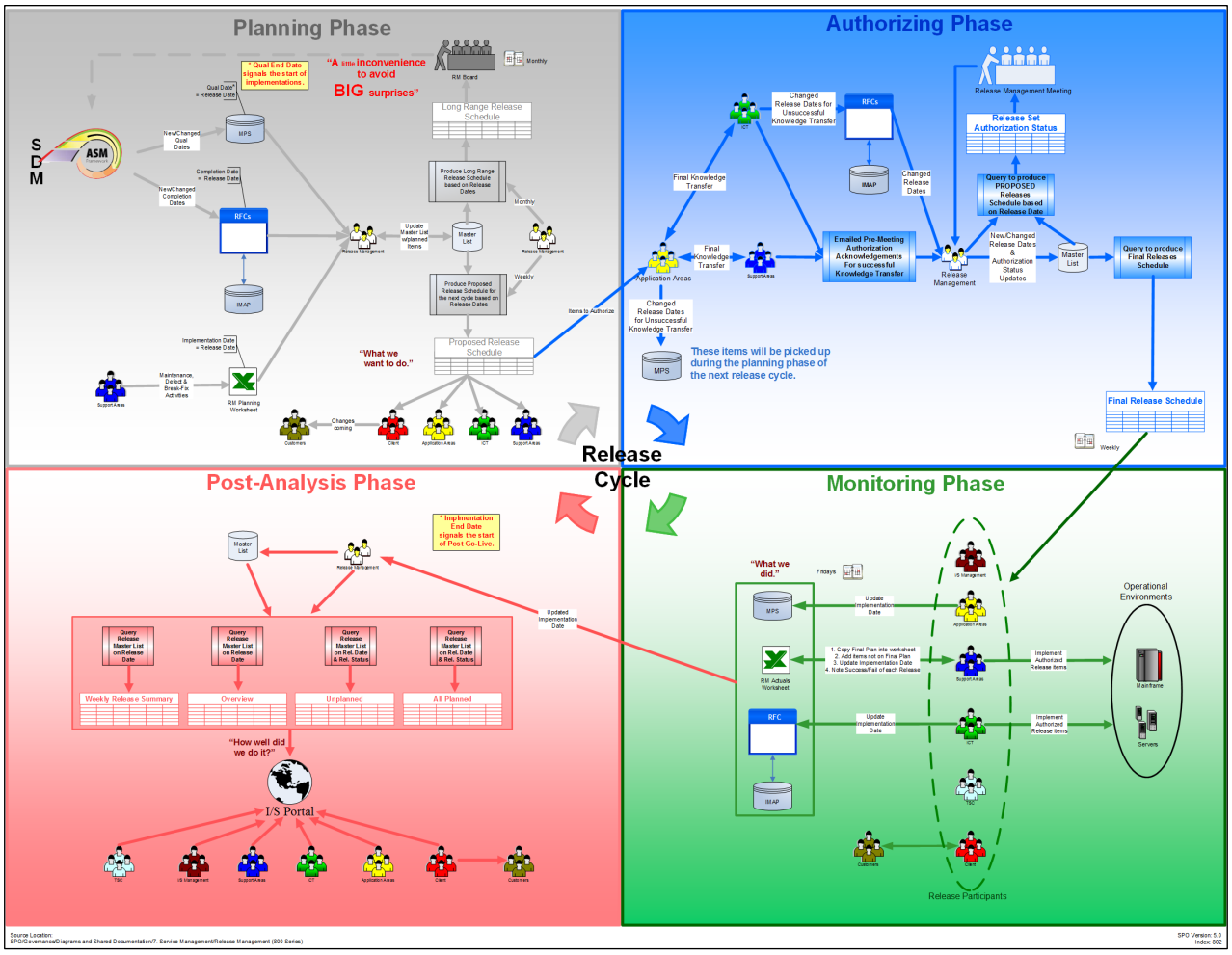


Figure 2-7 Release Management Release Cycle

The I/S Release Management (ISRM) serves two purposes: the first is provide support of the day to day Release Management activities; the second is to report on the participation and compliance to the Release Management procedures.

Figure 2-8 on the next page shows a calendar for the typical Release Cycle. It is important to note that activities from each phase actually occur throughout the week; however, the purpose of this representation is to depict the deliverables of each phase. Also, this calendar is a bit irregular as the week consists of eight days. *While Monday is the end of current cycle, it also represents the start of the next cycle.* This overlap allows for the routine weekend system maintenance releases to be reported.

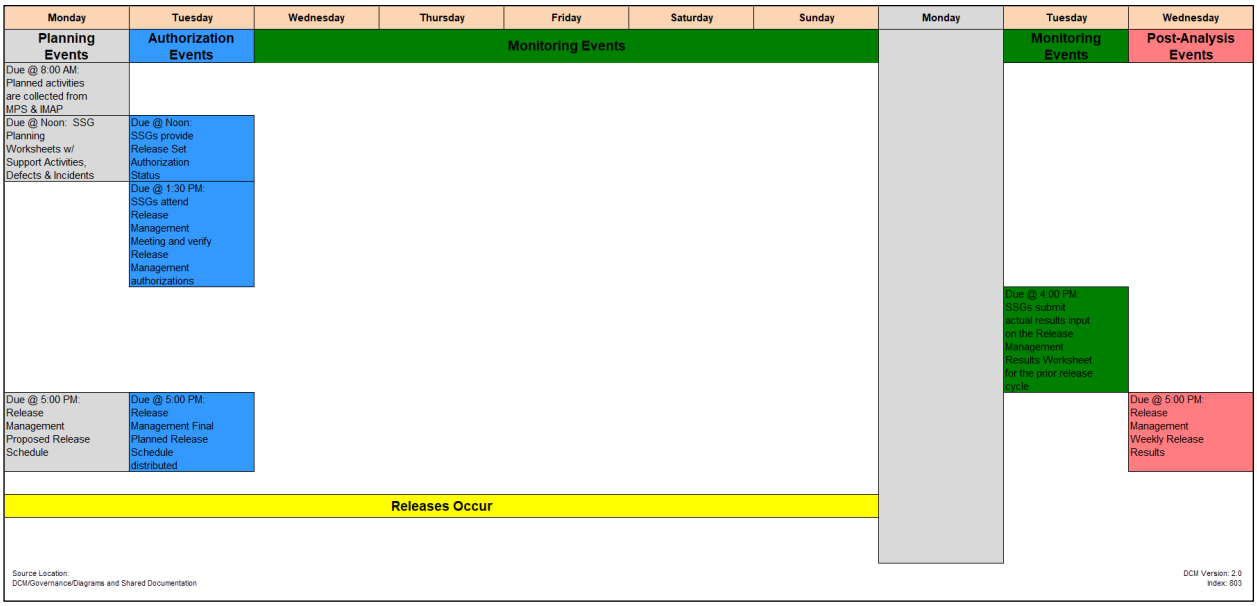


Figure 2-8 Release Cycle Calendar

NOTE The second Monday is technically the start of the next Release Cycle even though there are deliverables from the previous Release Cycle.

On the first Monday of each Release Cycle, all System Support and ICT Operational areas need to submit the Break/Fix and Maintenance items to be implemented into operational or deployed environments during that Release Cycle in the SSG Worksheet provided by Release Management. The ISRM will use that as well as collected data from MPS & IMAP to produce the Proposed Release Schedule.

On Tuesday, the System Support and ICT Operational areas are to provide the authorization status for all release items assigned to their group by the end of the Tuesday meeting. The ISRM will create a Final Release Schedule for all items that have been reported through the end of the Tuesday meeting.

On Tuesday of the following Release Cycle, the System Support and ICT Operations areas will use the Final Release Schedule (distributed by the ISRM) to mark the success of each Release Item. Also, the SSGs and ICT Operations should add any items implemented that were not on the Final Release Schedule. The ISRM will use this information to create operational reports identifying what was done and how well we did.

Additionally, I/S Release Management Long Range Planning is the gathering and communication of all known and/or anticipated work efforts that will either affect and/or be implemented into BlueCross Production environments. This encompasses all support and operational areas of I/S as well as review

and input from Project Management Office (PMO) and Client Management organizations. The continuous focus on planning contributes to stability in the Production environments. Long Range Planning contributes to the reduction of adverse impacts of incidents and problems for the business.

Below is a more high-level explanation for each phase of the Release Management process:

2.4.2.1 Planning Phase Highlights

The Planning Phase is the first phase of the Release Cycle for the Release Management process. This phase collects release items that need to be communicated to the **System Support and ICT Operational areas** for implementation and support. The planning that occurs during this phase is done with two objectives in mind: a weekly view for current issues and a long-range view for advanced notice both ensuring that resource conflicts are avoided and release items are implemented as scheduled.

The items in this phase are broken down and reported in four groups:

- **Scheduled** — All items collected from MPS, IMAP and Support/Maintenance activities from the SSG Planning Worksheet each Release Cycle.
- **Break/Fix** — All items collected from the System Support Planning Worksheet or reported via the Release Results Report for Break/Fix activities or incidents (Incident ticket number should be provided).
- **Post Go-Live** — All items collected from the System Support Planning Worksheet or reported via the Release Results Report for releases occurring during the Post Go-Live Phase defined in MPS for the effort.
- **Unexpected** — All items released that were not properly identified in MPS or IMAP.

Inputs

- Management Practices System (MPS) containing Work Requests (Projects & Change Sheets).
- Items in the Infrastructure Modification and Approval Process (IMAP) containing requests for change to the I/S infrastructure.
- System Support Worksheet containing release Items identified as ready for implementation.

Outputs

- Proposed Release Schedule containing Release Items that have been collected through the Planning Process for the current Release Cycle.
- Planning Pipeline containing Significant (identified in Planning Phase section) Release Items that have been collected for future Release Cycles.

2.4.2.2 Authorization Phase Highlights

The Authorization Phase is the second phase of the Release Cycle for the Release Management process. This phase identifies whether the System Support Group has received the proper knowledge transfer to accept responsibility for support of the implemented items. The Authorization Phase is an integral part of the Release Management process, as it is designed for **System Support and ICT Operational areas** to ensure that only quality items are released into the production/deployed environments.

The items in this phase are broken down and reported in two groups:

- **Execute** — System Support or ICT Operational area acknowledges the release item is ready to be released during the current Release Cycle.
- **Pending** — System Support or ICT Operational area has not acknowledged the release item is ready to be released during the current Release Cycle.

Inputs

- System Support or ICT Operations Authorization status communicated to the ISRM.

Outputs

- Final Release Schedule containing all authorized Release Items for the current Release Cycle.

2.4.2.3 Monitoring Phase Highlights

The Monitoring Phase of the Release Management process is the third phase of the Release Cycle and identifies all release items the System Support and ICT Operational areas have attempted to introduce into the production/deployed environments.

The items in this phase are broken down as follows:

- **Successful** — System Support or ICT Operational area indicates that the scheduled release item was introduced and now resides in the production or deployed environment.
- **Failed** — System Support or ICT Operational area indicates that the scheduled release item does not reside in the production or deployed environment. This can occur for one of the following reasons:
    - **Backed Out** — The release item was introduced into the production or deployed environment but was removed due to errors or problems.
    - **Partially Successful** — The release item was introduced into the production or deployed environment, but not 100% of the release item resides in production.
- **Not Attempted** — System Support or ICT Operational area indicates that there was not an attempt made to move the scheduled release item in the production or deployed environment.
    - **Cancelled** — The effort has been terminated.
    - **Rescheduled** — The release item was scheduled but was not introduced into the production environment during the current release cycle. It has been scheduled with a new, future release date.
    - **Withdrawn** — The release item was schedule but was not introduced into the production environment during the current release cycle. It will be scheduled for a future date to be determined or has been previously released.
    - **Moved Previously** — The release item was introduced into the production or deployed environment in a previous release cycle.
    - **Stopped** — System Support or ICT Operational area stopped the move from occurring.
- **None Provided** — System Support or ICT Operational area did not provide a required response for the result of the release item.

Inputs

- Final Release Schedule containing all authorized Release Items for the current Release Cycle.

Outputs

- RM Release Results worksheet containing the scheduled Release Items, unexpected (not scheduled) Release Items, Break/Fix Release Items and Post Go-Live Release Items.

2.4.2.4 Post-Analysis Phase Highlights

The Post Analysis Phase of the Release Management process is the final phase of the Release Cycle and identifies how the I/S Organization is performing the previous three phases.

Inputs

- Release Management Master List containing all of the historical data as a result of performing the Planning, Authorization and Monitoring Phases.

Outputs

- Various performance and trending reports containing data representing an I/S Organizational or Application Area view of the Release Management activities with month-to-date and year-to-date metrics.

2.5 Configuration Management

2.5.1 Configuration Item Management

The processes that provide direct control of I/S Assets related to Application Systems and Information and Communication Technology (ICT) and Infrastructure Configuration Items (CIs) used in the provision of live, operational services are referred to as **Configuration Item Management**.

Configuration Items are any component of an Application System and ICT infrastructure, including documentation, which is (or is to be) used in the provision of live, operational services. The lowest level CI is normally the smallest significant unit that will be changed independently of other components. CIs may vary widely in complexity, size and type, from an entire database to a single program module or a minor hardware component.

The determination of what constitutes an individual CI is the responsibility of the organization supporting the CI and must take into account all aspects of the configuration management standards.

NOTE The following Configuration Item Management standards are to be applied with discretion weighing the cost of compliance versus the resultant business value. The application of these standards on a case-by-case basis must take into account the following characteristics of a given Configuration Item, which will determine the business value of full compliance:

- Frequency of change or update.
- Volume of inventory.
- Amount of interaction or overlap with other areas.
- Criticality of use.

If one or more of these standards are not identified to have sufficient business value, justification must be provided and a standards waiver requested for each occurrence via the Waivers to Standards process. Refer to *Adaptive Change* > *Process Audit* > *Waivers* for details.

2.5.1.1 Standards Overview

As illustrated in Figure 2-9 below and described in detail in the sections that follow, there are eight categories of standards for Configuration Item Management: Identification, Control, Status Accounting, Verification, Reporting, Recovery, System Documentation and Security. Each category has a given definition and an established standard or standards.

NOTE For all CIs, there need to be specific standards in place that address each of the general standards discussed within.

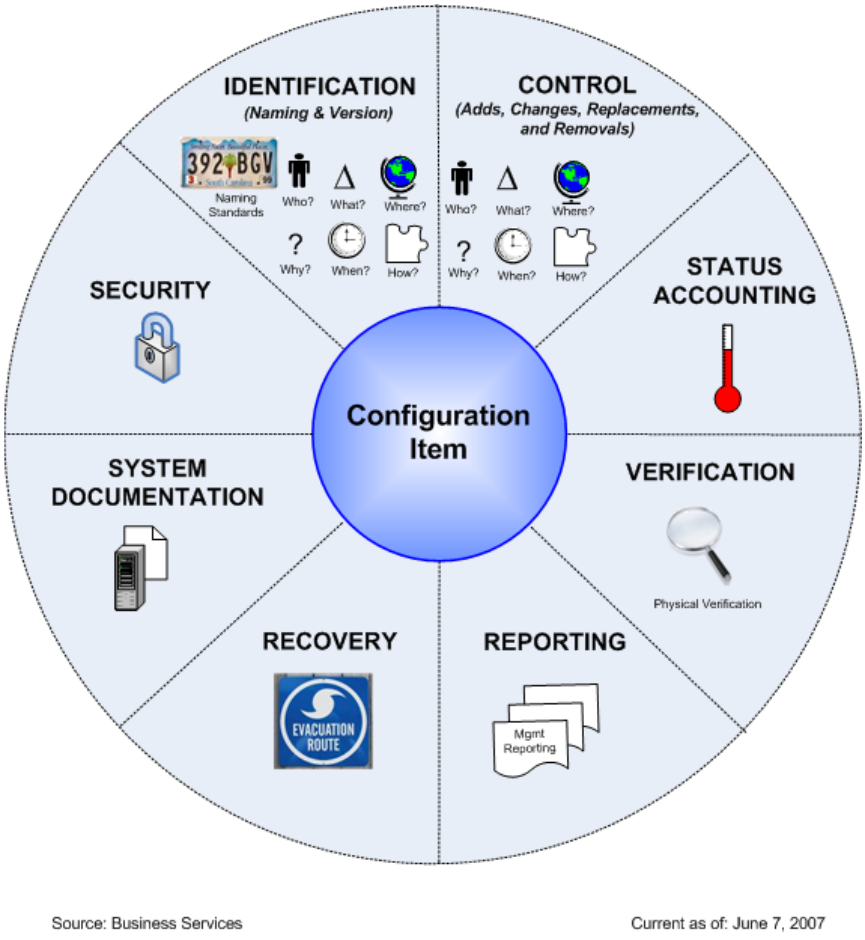


Figure 2-9 Configuration Management Standards

Identification

The processes that define and maintain naming conventions and version numbers of Configuration Items (CIs) are defined as Identification.

- **Standard**: Each CI has a documented Information Systems Standards Manual (ISSM) approved naming and versioning convention.
- **Standard**: The addition, change, replacement or removal of a CI is uniquely identified regarding who, what, when, why, how, and where it was changed through ISSM-approved tools and repeatable processes.

Control

The processes that ensure no Configuration Item (CI) is added, changed, replaced, or removed without appropriate approval and documentation are defined as Control.

- **Standard**: All adds, changes, replacements, or removals occur under ISSM-approved tools or repeatable processes that enforce the Configuration Management standards requiring approval prior to any change to occur to a Configuration Item (CI).
- **Standard**: All approval processes occur under ISSM-approved tools or repeatable processes that enforce the creation and retention of approval documentation related to any change to occur to a Configuration Item (CI).

Status Accounting

The processes that establish track and store the current and historical Configuration Item (CI) status during its life cycle (from birth to death) are defined as **Status Accounting**.

- **Standard**: All adds, changes, replacements, or removals occur under ISSM-approved tools or repeatable processes that record and retain a standard set of current and historical status levels related to each Configuration Management Control activities that take place.

NOTE For example, Application Systems CIs may have a status of active or inactive. Examples of ICT Infrastructure CI statuses may be under development, planned/ordered, received/in-stock, installed, tested, implemented, operational, maintenance, spare, phase out, removed, or stolen.

Verification

The processes of auditing the set of Configuration Management data stores against the actual physical existence and status of the Configuration Items (CIs) are defined as **Verification**.

- **Standard**: To have ISSM-approved and repeatable processes to perform the verification of the Configuration Management data stores against the physical implementation.

Reporting

The processes of producing management reports from Configuration Management data stores are defined as **Reporting**.

- **Standard**: To have ISSM-approved and repeatable processes to ensure the ability and accessibility for other processes to produce management reports in a timely fashion to meet demand.

Recovery

The processes to restore the Configuration Items (CIs) from a point of failure back to its intended use are defined as **Recovery**.

- **Standard**: To have ISSM-approved and repeatable processes to ensure the appropriate version of a Configuration Item (CI) can be recovered within an agreed upon time period. The agreed upon time period (Recovery Time Objective — RTO) is established between the CI support organization and the users of the Configuration Item (CI)

- **Standard**: To have ISSM-approved and repeatable processes to ensure the appropriate version of a Configuration Item (CI) can be recovered back to an agreed point in time. The agreed point in time (Recovery Point Objective — RPO) is established between the CI support organization and the users of the Configuration I.

System Documentation

The documentation that furnish a high-level overview reflecting the current state of the CI and that create a knowledge base to make a modification, fix an error or to accommodate a new requirement are defined as **System Documentation*.**

- **Standard**: To have ISSM-approved and repeatable processes to ensure the creation and maintenance of required System Documentation.

Security

The processes in which security requirements are incorporated to ensure conformance with applicable regulations, policy, requirements, and to identify potential relevant risk areas and recommend risk mitigation measures are defined as **Security**.

- **Standard**: To have ISSM-approved and repeatable processes to ensure Configuration Management Standards and mitigate conformance with the applicable regulations, policy, requirements, and to identify potential relevant risk.

NOTE These standards have been based on Application Systems and ICT Infrastructure. Consideration of Life Cycle Documentation will be incorporated into these standards at a future time.

2.5.1.2 Workstation Variation

The manager that is responsible for the deployed Workstation CI is also responsible for reporting any adds, changes, replacements, and/or removals of the Workstation CI to Workstation Support.

2.5.1.3 Software Configuration Management

The Software Configuration Management (SCM) Department, part of the Internal I/S Support area, administers the tools used by I/S to manage software configuration items.

The SCM Department is responsible for coordinating the approval, establishment, and implementation of all development and testing environments for Host and Non-Host development. This includes Customer Information Control System (CICS) regions, DB2 subsystems, IMS subsystems, z/OS Linux servers, and system-related elements such as compilers, operating systems, and other system software.

The development areas involved will be responsible for coordinating the use of the environments that have been assigned to them.

Over time, terms used to describe both testing regions and validation techniques have evolved. A problem arises when the same word is used to describe both a validation region and a validation technique. The two most common words confused are Unit and System Test. For example, Unit Test, is at times used to describe the region where validation occurs and at other times to describe the process of validating individual components of a program. Therefore, it is important to distinguish the difference between where a validation occurs and the nature of the validation itself.

This is complicated due to the complex nature of applications supported as a company and the different users of those systems. For example, internal users are clients and external users are called customers. The user interface can be an Enterprise Server direct connection or more frequently a graphic user interface through a client PC. This introduces the mixing and matching of test regions on the Enterprise Server and the servers that render pages to a user. A unit test server may actually be pointed to the QA region on the Enterprise Server.

2.5.2 Introduction

2.5.2.1 Program Overview

Configuration Management consists of four separate tasks: identification, control, status accounting, and auditing. For every change made to an Automated Data Processing (ADP) system, the design and requirements of the changed version of the system should be identified. Subjecting every change to documentation, hardware, and software/firmware to review and approval by an authorized authority performs the control task of Configuration Management. Configuration status accounting is responsible for recording and reporting on the configuration of the product throughout the change. Finally, through the process of a Configuration Audit, the completed change can be verified to be functionally correct, and for trusted systems, consistent with the security policy of the system. Configuration Management is a sound engineering practice that provides assurance the system in operation is the system supposed to be in use. The assurance control objective as it relates to configuration management of trusted systems is to guarantee that the trusted portion of the system works as intended.

Procedures must be established and documented by a configuration management plan to ensure that configuration management is performed in a specified manner. Any deviation from the configuration management plan could contribute to the failure of the configuration management of a system entirely as well as the trust placed in a trusted system.

2.5.3 Purpose

The purpose of Configuration Management is to ensure changes to existing ADP system takes place in an identifiable and controlled environment and that they do not adversely affect any properties of the system, or in the case of trusted systems; do not adversely affect the implementation of the security policy of the Trusted Computing Base (TCB). Configuration management provides assurance that additions, deletions, or changes made to the TCB do not compromise the trust of the originally evaluated system. It accomplishes this by providing procedures to ensure that the TCB and all documentation are updated properly.

2.5.4 Policy

The two major TCB components in use at BlueCross BlueShield of South Carolina (BlueCross) are the IBM Resource Access Control Facility (RACF) and the Microsoft Active Directory system. Both of these

security products have been evaluated by the National Security Agency (NSA) as being totally compliant with C2 level of security. Further, with some setting of security label controls, the RACF system is certified to the B1 level of security. It is imperative that any changes to these two TCBs be closely monitored through the configuration plan to ensure that changes made do not compromise these levels of security. The RACF passwords are encrypted.

2.5.5 Objectives

BlueCross provides compliance with the scope and objective of the National Computer Security Center's guidance on configuration management, which enhances system stability and security features.

2.5.6 Scope

This plan is a result of requirements involving the TRICARE contract. Although this plan is driven by these contract requirements, a similar plan has been in use at BlueCross for a long time and is referred to as the "Problem and Change Management Overview and Procedures" manual. This configuration management plan encompasses the requirements of the "Problem and Change Management Overview and Procedures" and information contained in NCSC-TG-006-88.

2.5.7 Management Meetings

There are four types of meetings included within the Configuration Management Plan:

- The first meeting, the **Daily 8:15 Meeting**, is conducted daily at 8:15 and attended by Information Systems (I/S) Management.
    - The previous day's problems in both batch and online applications are reviewed. The Vice President of Information System Operations determines when to escalate a problem to the **Critical Situation Meeting** for resolution.
- The second meeting, a **Weekly QA Meeting**, examines problems in exception status (those that have not been resolved within the specified time period for the severity assigned) and to review their action plans and severity.
    - The availability and stability of the system for the previous week is reviewed to determine whether any trends are developing that should be investigated. The statuses of all open changes are reviewed.
    - **Each submitting department conducts this second meeting.**
- The third meeting, the **Weekly Change Meeting**, obtains management approval for change scheduling, review and confirm the change schedule, and to resolve any scheduling conflicts.
    - Invited attendees of the Weekly Change Meeting include:
        - Director, Technical Support or Designee
        - Director, Information Systems Operations or Designee
        - Director, Database Administration or Designee
        - Director, ICT Non-Host or Designee
        - Director, LCAS Non-Host or Designee

  - Director, LCAS Host or Designee
  - Change Manager, Change Management or Designee
  - Representative, IT Business Systems (ITBS) or Designee
  - Client Managers or Designees

- The fourth meeting, the Critical Situation Meeting, is conducted after a significant outage has occurred.

  - The purpose of this meeting is to review the outage to determine if the appropriate actions were taken to reduce the impact of the problem.
  - The results of this meeting are documented and reviewed with senior-level data processing management.

The effectiveness of the **Configuration Management Plan** is measured by:

- Reviewing the established objectives to ensure implementation was conducted in a timely manner.
- Ensuring system security controls were not compromised.
- Verification that adequate documentation was completed to record any system upgrades.

2.5.8 SharePoint Online

2.5.8.1 Introduction

SharePoint Online (SPO) is a tool used to share and collaborate with colleagues, partners and customers. It allows groups to set up a centralized, secure space for document sharing, editing and downloading.

The documentation generated and used by our organization in the execution of our day-to-day work is viewed as corporate assets, and to that end requires formal management procedures.

For the purpose of defining these standards, **documentation** is defined as any electronic object whether generated by software or scanned.

NOTE Software code, software configuration elements, executables, and databases do not fit the definition of documentation generated by software and are prohibited from being stored in ***SPO***.

SPO is hosted by Microsoft in the Cloud.

The ***SPO*** standards do not deal with the content, form or style of documentation, but rather with controlling the factors regarding its physical existence. However, everyone is urged to be attentive to legibility of all documentation. In general, the recommended minimum font size is 10 points.

The standards address the required elements of Configuration Management:

- Identification
- Control

- Status Accounting
- Verification
- Reporting
- Recovery
- System Documentation
- Security

2.5.8.2 Governance

The I/S Policy Committee determines the approved uses for ***SPO*** within I/S. Once a new category of documentation is approved, standards should be developed for that category and published in this section of the ISSM.

The R&D Committee and/or the Solution Detail Review Process (SDRP) Committee approve both the customer uses of ***SPO*** and the functionality available within ***SPO***.

The following topics describe approved documentation categories for ***SPO***.

Work Request Life Cycle Documentation

Work Request Life Cycle Documentation provides the means to review Work Requests for reasons ranging from continuous improvement activities to legal requirements. It is vital that all information is preserved and organized to facilitate successful reviews. Work Request Life Cycle Documentation consists of the documents that provide evidence of the activities described in:

- Work Request process workflows. Refer to the methodology diagrams in *Application Systems Management > Application Systems Management Framework*.
- System Development Methodologies.
- Research and Development.
- Request for Solution (RFS).
- Audit Requests.
- Other.

In other words, they are the documents normally stored in a project book or change sheet folder.

Automated methodology approvals are not captured by ***SPO***. Rather, as defined in the formal Work Request methodology, evidence of approval is captured and stored within a methodology document or other documents. For example, approval emails and scanned approval signatures.

Documentation Content

Content will vary depending upon the details of the Work Request. It should contain all relevant documentation that would be beneficial in understanding what has transpired during the Work Request.

The following is a sample of potential contents:

- Copy of the Work Request established for the Project or Change Sheet
- JRP Documentation
- JAD Documentation
- Completed Test Plan

- Completed I/S Test Matrix
- Work Request Status Reports
- Change Control Documentation
- Costing Documentation
- Copies of Significant Email Messages
- Task Lists & Project Plans
- Bridge Diagram
- Security Compliance Acceptance Review
- Issues Log & Related Emails
- Purchase Request Packets

There is no formal walkthrough for the Work Request Life Cycle Documentation. This documentation is maintained and stored in ***SPO***.

I/S Departmental Documentation

SPO sites may be created for each department within I/S. By default, access to these sites is restricted to the members of that department. This is to prevent the unintended use of departmental documentation by areas for which it was not intended. Information that applies across departments should be published in an accessible location such as the Management Practices Manual (MPM) or the Information Systems Standards Manual (ISSM).

I/S Governance Documentation

All master files of I/S Governance documentation reside and are maintained in ***SPO***. I/S Governance documentation includes the ISSM, Guiding Principles & Concepts, Organizational Structure & Processes, the System Architecture Book, the Managing People Program, and all of their included supporting diagrams and charts. The I/S Standards Committee, the I/S Policy Committee, and their respective subcommittees store and manage their documentation in their corresponding ***SPO*** sites. This documentation includes agendas, meeting minutes, task lists, white papers, ISSM updates, and any other subcommittee-related documentation.

System Documentation

System Documentation includes the application system documentation, such as Concept Diagrams and Disaster Recovery Plans, that is required by the standards in *Technical Standards — Infrastructure > Overall Technical Infrastructure Standards*. This documentation category also includes any other documentation that exists about an application system, such as vendor documentation, user manuals, etc.

I/S Administrative Artifacts

The documentation category of I/S Administrative Artifacts includes other documentation that is created within I/S for use within I/S. Currently approved uses are:

- Cost & Budget Committee Documentation — The I/S Cost and Budget Committees use their ***SPO*** sites to store and manage documentation relevant to their charters and committees. Access is restricted and accessible to identified personnel only.

- Business Continuity Plans — The Business Continuity (BC) Plans that are stored in ***SPO*** are an output of the Assurance website and managed by the BC administrator. The BC Plan maintenance continues in the Assurance website.

2.5.8.3 Standards and Guidelines

General

Identification

Metadata Fields

A minimum set of metadata fields must be populated for the purpose of identification. The following metadata fields are generated by the system and cannot be altered:

- Created (Time and date stamp)
- Created By (person who created the document in ***SPO***)
- Modified (Time and date stamp)
- Modified By

Additional metadata fields can be defined for any documentation category by site owners if necessary.

File Naming Guidelines and Restrictions

Each file name must be descriptive of its content and remain static so that the application can manage and increment the document versions. The inclusion of dates in a file name is acceptable only for reporting documentation (e.g., status report, agenda, or recap) to reflect a specific status for a specific point in time.

NOTE Including the document status in a file name (e.g., *revised*, *draft*, *final*) is not acceptable and disrupts the ***SPO*** version control methodology. We encourage users to not require checkout of documents as this prevents users from collaborating real time with other editors.

Do not save a new version of a document with a new name. This disrupts the version management of the original document and makes it difficult to determine which document is the current one.

The following file naming restrictions are system limitations and apply to all documentation stored in ***SPO***:

- File name must not exceed 128 characters.
- The following characters cannot be used: " # % & * : < >? \ / { | } ~
- The period character cannot be used in the following ways:
  - Consecutively in the middle of a file name (…)
  - At the end of a file name (after the file type extension)
  - At the beginning of a document name

Control

All documentation categories defined in subsection *Governance* above must be housed and managed within ***SPO*** so it can be retrieved by anyone who has been granted access to the documentation.

The master copy of each piece of documentation will reside within one library of ***SPO***. Duplication of documentation within ***SPO*** is not allowed.

Documentation Distribution/Sharing

Documentation is shared by sending a URL that points to the documentation.

Example URL: https://WebApplicationRoot/sites/GS1070/Scope/GS1070_Scope.docx

Documentation distribution by email attachment is prohibited unless there is no other alternative. For example, it is permissible to send an attachment to a third-party contractor who has not established access to ***SPO***.

Administration

Day-to-day administrative functions of ***SPO*** for I/S are handled by the ***SPO*** System Administrator.

Selected administrative functions can be extended to specific user roles. The extent and nature of this extension is determined by the business needs and use defined for each documentation category housed within ***SPO***.

Documentation References

URLs are used externally to reference documentation in ***SPO***.

Hyperlinks within Work Request sites are prohibited when linking from one document residing in an ***SPO*** Work Request site to another document within an ***SPO*** Work Request site.

Recovery

Recovery procedures and objectives are provided in the Disaster Recovery Plan for the ***M365*** system.

System Documentation

Documentation and training are available on how to use ***SPO***.

Security

SPO shall limit access to documentation in compliance with government and corporate requirements. At the same time, it shall be possible to grant access to any user who has a business need.

Documentation access is controlled by defined entities as required by the business need. Access is controlled by either Active Directory and ***M365*** groups or the Site Permissions function within ***SPO***.

2.6 Inventory Management

2.6.1 Software Reviews

Process Audit (PA) conducts two parallel reviews of software: a monthly review of only the Medicare network for unauthorized personal computer (PC) software, and a quarterly review of the SMI data with the applicable owners. The monthly review uses discovery data to compare the list of software currently installed on workstations within BlueCross BlueShield of South Carolina (BlueCross) to the software listed in the System Master Index (SMI). PA reviews the installed PC software not listed in SMI ("discovered software") and works to determine if it matches an approved software item, needs adding to SMI, or requires removing from the PC. The quarterly review validates the data recorded in SMI to ensure proper control, ownership and stewardship of all BlueCross software.

NOTE This does not refer to the reconciliation of installed software to software licenses.

2.6.2 Software Compliance Audits

The periodic software reconciliation of titles under management performed by Software Asset Management compares the authorized quantity of purchased software entitlements for a given software title with the actual current usage of that title by BlueCross systems. If the software reconciliation determines that the entitlement quantity of a software license falls short of the current usage, the responsible technology owner (TO) must either arrange to remove a sufficient quantity of the installed software to maintain compliance or initiate a purchase requisition (PReq) to acquire additional entitlement capacity to maintain compliance.

2.6.3 Infrastructure Hardware Cyclical Inventory

BlueCross maintains a centralized repository of physical information technology (IT) components (both owned by BlueCross and entrusted to BlueCross) in the ***IBM Control Desk (ICD)*** — the system of record for IT assets — to support our business within the authorization boundary of the information system. The ***ICD*** equipment inventory records and related reports also contribute to processes in other departments.

Representatives from Acquisition and Inventory Management Services (AIMS) and ICT Operations perform the inventory process of the fixed and durable IT equipment in all locations of the BlueCross environment at least once per calendar year. AIMS will conduct a separate cyclical inventory of the contents of their secure storerooms.

NOTE Fixed IT equipment is a serialized trackable asset (has an ***ICD*** asset ID) that can or may have an ***Infrastructure Designer (IaaSD)*** ID and is subject to maintenance (e.g., major component end items

---

such as a PC or a server).

Durable IT equipment is a serialized trackable asset (has an ***ICD*** asset ID) that does not have an ***IaaSD*** ID but is subject to maintenance or other specific business considerations. An example of durable IT equipment would be the hard drive in a PC or a server.

The representatives performing the physical inventory will use data extracted from the systems of record (e.g., ***ICD***) for the area to inventory (e.g., printout by room in rack# order).

Inventory deliverables by the representatives include:

- Archive the incremental results of cyclical physical inventory on the network.
- Reconcile the physical inventory results to the systems of records (e.g., ***ICD***, ***IaaSD***).
- Document the resolution for the discrepancies found in each phase of the annual inventory.

At the completion of the physical inventory for a given year, the representatives from AIMS and ICT Operations will compile a completion memorandum summarizing the results and send the memorandum to operational stakeholders, financial stakeholders. senior management stakeholders, and executive stakeholders.

2.6.4 Infrastructure Decommission

The ***Integrated Cloud Orchestration System (ICOS)*** contains detailed records of both the deployment of infrastructure components and their decommission.

2.6.5 Missing Equipment

If after appropriate due diligence, I/S Asset Services (AS) cannot determine the location of an infrastructure asset with the assistance of the Owners, the Systems Health Analysis Reporting and Estimating (SHARE) team, Inventory Management, ICT Operations, and Facilities, then BlueCross considers the asset missing. Then, in accordance with the protocol from the Cybersecurity Operations (SecOps) team, AS initiates a ticket to SecOps reporting a missing asset and includes with their report the collected research documentation. SecOps presents the results of their formal investigation to the appropriate managers and AS.

2.6.6 Resource Acquisition Standards

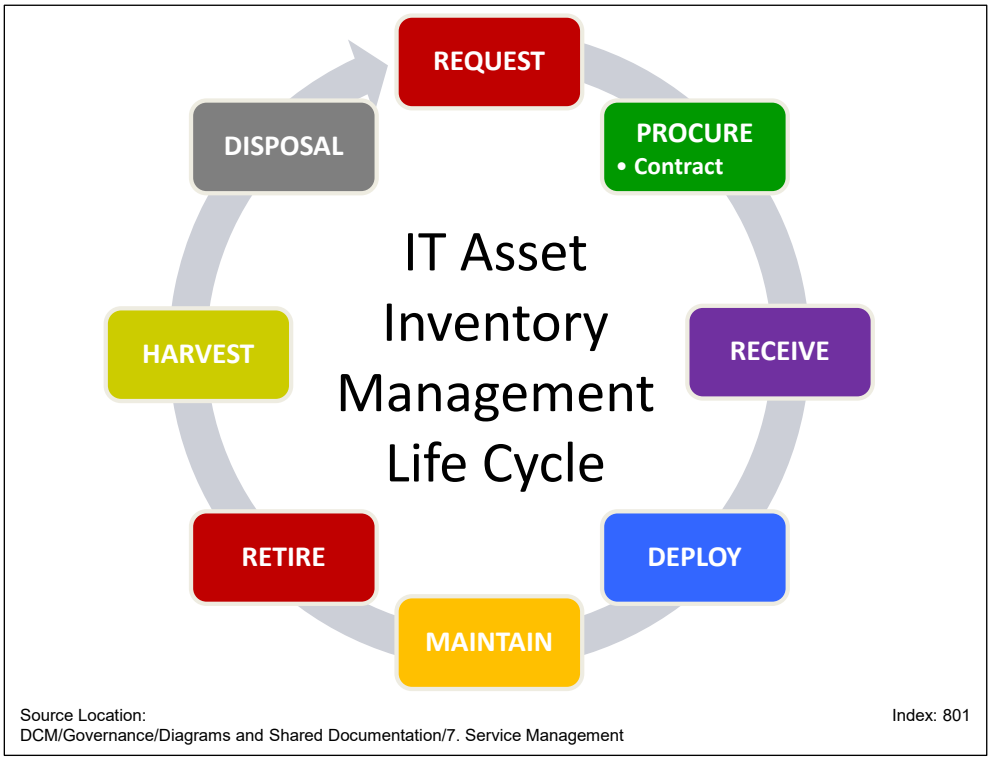


Figure 2-10 IT Asset Inventory Management Life Cycle

2.6.6.1 I/S Acquisition Overview

The AIMS Department provides the primary point of contact for IT assets. The AIMS subdepartments issue purchase orders, write contracts, receive purchases, account for Information Technology (IT) assets, and maintain the data related to the IT assets for all IT hardware, software, services, and maintenance for BlueCross and its subsidiaries.

The IT Asset Inventory Management Life Cycle (Figure 2-10) begins with the submission of a document containing a list of resources needed by a Line of Business (LOB) and the legal authorization to spend money to acquire the resources. For details, refer to *LOB Management* > *Resource Acquisition* > *Requesting Resources*.

If purchasing an information system component, the owner of the information system must sign the documents to acknowledge the assignment of the component to the information system.

With the exception of direct reports to the Chief Executive Officer (CEO), management may not approve disbursements or a request for resources for themselves or payable to other entities on their OWN behalf (Corporate Policy 65286 — Fiscal Disbursement). Some types of expenditures require additional authorization, regardless of position. Refer to Corporate Policy 65284 — Purchasing and Corporate Policy 65286 — Fiscal Disbursement for such expenditures.

2.6.6.2 Delegation of Signature Authority

Direct Reports to the CEO may delegate higher authorization levels to specific employees for specific business purposes, not to exceed the $100,000 limit (Corporate Policy 65286 — Fiscal Disbursement). All other exceptions to the limits outlined in Corporate Policy 65286 — Fiscal Disbursement must be requested in writing and be approved by the Chief Financial Officer (CFO). I/S Procurement (ISP) files the approved exception documentation on the department's ***SharePoint Online (SPO)*** site.

2.6.6.3 I/S Acquisition Guidelines

The AIMS subdepartment ISP accepts only spending authorization signatures in accordance with the corporate signature-level requirements in Corporate Policy 65286 — Fiscal Disbursement (see previous section for details). All requests for an exception to the standard amounts listed in the Fiscal Disbursement policy must be forwarded to the Chief Information Officer (CIO) for approval.

The justification information helps I/S maintain accurate costing and helps to better understand and categorize I/S purchases in terms of the *driving event* that precipitated the purchase.

ISP promptly processes newly received requests using the purchasing system — ***IBM Control Desk (ICD)***.

All Acquisition Specialists seek competitive Requests for Quote (RFQ) from responsive and responsible sources. The considerations for prospective sources of supply include — but are not limited to — financial status, government requirements, General Services Administration (GSA) Pricing, Federal Debarred List, Anti-Terrorist Act, and acceptance of applicable flow-down clauses.

Acquisition Specialists determine awards based on cost, service, Small and Disadvantaged Business (SADBUS) utilization, Single Source, or other documented reasons.

By policy, BlueCross ensures that none of the supplies or materials furnished for our contracts are *suspect or counterfeit parts*. BlueCross uses only vendors/suppliers properly registered via the I/S supplier registration process. ISP documents accurately characterize the status of any parts purchased (whether new, used, or refurbished) to prevent even the impression that they are of a different class or quality, or from a different source than is actually the case. The receiving process also verifies that the goods received match the issued purchase order. Once issued to operations and prior to being deployed into a production environment, software and hardware are placed into a test environment for assessment.

2.6.6.4 Provisioning a New Hire

The responsibility for providing new hires a PC resides with the new employee's LOB manager. Use equipment from the LOB department's inventory before requisitioning additional equipment from I/S inventory. All new PCs (desktops, laptops, or virtual) require software licenses for the corporate standard software.

For new I/S positions, the I/S Space Coordinator arranges deployment of a configured, company-standard PC unless the hiring manager states that one is not required. This process is unique to I/S; all other areas order equipment as needed.

2.6.6.5 Receive

The responsibility for documenting the arrival of goods and the initiation of asset records belongs in the Receive Phase of the life cycle. IT Inventory Specialists compare shipment manifests (packing slips) to both the received items and purchase orders (PO) to ensure that the company gets the authentic goods ordered and allow Accounts Payable to promptly pay invoices. Other key Receive Phase responsibilities include but are not limited to the following:

- Receive into purchasing system (***ICD***) storeroom for hardware (tangible items) and software module for software (intangible items).
- Create asset tags and apply them to trackable assets.
- Log hours provided by business units for services.
- Inspect newly arrived boxes for damage and return to the vendor any items damaged in shipment.

2.6.6.6 Deploy

The company stores its tangible stock of inventory (rotating) and non-inventory (non-rotating) items in secure locations. The ***ICD*** software module contains the documentation of the company's software entitlements (intangible goods). Filling requests from the company's stock of equipment occurs during the Deploy Phase of the life cycle. The IT Asset Specialists direct the issuing of items; the IT Inventory Specialists perform and document the issuing of the items. Issuing nonexpendable property (items with an asset tag) requires documentation of the chain of custody to ensure positive accountability of these numbered assets. The signatory retains personal responsibility for the asset until signed for by another person. Durable and expendable property items require only a simple signature not the full chain-of-custody documents when issued. Issuing software involves an IT Asset Specialist linking a software entitlement in the library to an operational asset by the Configuration Item (CI) name of the appropriate physical device or logical instance, which allows the use of the software. Unlinked entitlements again become available for issue.

NOTE A durable property item is an item that is not consumed in use, and keeps its original identity (e.g., a keyboard or a mouse). If not classified as durable, a property item that is consumed in use or loses its identity in use is classified as expendable (e.g., a video card once it's installed in a PC).

Once custody of the items transfers, the technicians prepare the items for operation.

The IT Inventory Specialists issue items to support Break/Fix repairs (Incidents) to operational systems 24/7/365.

2.6.6.7 Maintain

The Maintain Phase involves maintaining records on all company assets for the life of the items. A Role involved in the Maintain Phase is the IT Asset Specialist. They perform cyclical comparisons to the reports from operational items to verify record accuracy. The IT Asset Specialists investigate any discrepancies and implement the appropriate fixes to ensure accuracy of ***ICD*** data. Maintain tasks include, but are not limited to the following:

- Software reconciliations performed annually on standard software and more frequently if required by contract — Task is performed by a Software Asset Manager (SAM).
- Cyclical inventory counts of stock items (unissued inventory) — Task is performed by an Inventory Control Specialist.
- Cyclical inventory counts of equipment issued for use (e.g., production, testing) — Task is performed by a Hardware Asset Manager (HAM).

2.6.6.8 Retire

The Retire Phase involves removing operational items from use when no longer required. Retiring physical items includes an evaluation by the Platform and Finance teams of the retired item's further usefulness and compliance with standards. If retired, the Platform team conducts and documents a security wipe, updates the chain of custody with the IT Inventory Specialists, and transfers the items to a storeroom (inventory). The Platform team maintains the required Sanitization Log, which is the official written record of sanitizing a specific unit at a point in time.

2.6.6.9 Harvest

The Harvest Phase delivers the company cost avoidance by reducing the need to buy more of the restocked items or entitlements. Making an entitlement still covered by support contract available for reuse by the company occurs during the Harvest Phase of the life cycle. Reusing software entitlements involves communication with the software IT Asset Specialists who unlink the ***ICD*** software module record from the named asset. Harvest of hardware involves returning complete equipment or extracted parts from equipment scheduled for disposal to the storeroom and making them available as stock (open inventory). The Harvest Phase loops the life cycle back to the Deploy Phase.

2.6.6.10 Disposal

Eliminating unwanted items from the company occurs in the Disposal Phase of the life cycle. The Disposal Phase involves the final destruction of sanitized storage media (e.g., hard disk drives, CD/DVD platters) and the liquidation of devices.

The IT Asset Disposition (ITAD) team maintains the chain-of-custody tracking log, liquidation records, and (for storage media) Certificates of Destruction for a minimum of five years on all items leaving BlueCross. IT Inventory Specialists upload all IT asset disposal records to the official electronic record system to ensure proper record retention at the end of the IT Asset Inventory Management Life Cycle.

Disposal information for other departments can be found in the following ISSM sections:

- *Technical Standards — Infrastructure > User Interfaces > Workstation Sanitization*
- *ICT Infrastructure Management > Operations Management > Infrastructure Support > Media Protection*

NOTE For additional information, refer to *LOB Management > Resource Acquisition > Contract Management*.

Chapter 3 Service Delivery

3.1 IT Service Continuity Management

3.1.1 I/S Crisis Management

Certain Break/Fix incidents based on their individual characteristics require extraordinary efforts to resolve or require special attention. Declaration of a Crisis is the responsibility of either the CIO or judgement from the Incident Management Process. A Crisis is declared based on Red Alert Triggers, which determine the need for the Crisis Management Process to be initiated.

The Crisis Management Team is engaged when a Crisis is declared. These are the phases of the Crisis Management Process:

- Initiate Crisis Management
    - In the Initiate Crisis Management Phase, the Crisis Management Team performs the following activities:
        - Builds the team and engages the appropriate Crisis Recovery Team
        - Builds the Action Plans to work the crisis
        - Builds the communication plans to communicate the progress to management
- Work the Crisis
    - In the Work the Crisis Phase, the Crisis Recovery Team performs the following activities:
        - Assigns and confirms tasks among the team
        - Performs the work and collects team statuses
        - Analyzes the situation and prepares the results
        - Determines if there's a potential disaster

NOTE If there's a potential disaster, the Crisis Recovery Team consults with the CIO to confirm the disaster. Once the disaster is declared, the Disaster Recovery Process is initiated. Refer to the remaining sections below for information on recovery procedures.

If the Crisis Recovery Team determines that there's no potential disaster, the team proceeds through the Work the Crisis Phase and communicates progress updates to management. At this point, the Crisis Recovery Team makes the decision to place the Recovery Vendor on alert. Once the Crisis Recovery Team determines that the Crisis is resolved, the team will proceed to close the crisis.

- Close the Crisis
    - In the Close the Crisis Phase, the Crisis Management Team coordinates the following activities:
        - Initiates closure activities

- Conducts a post-crisis analysis
- Conducts a Lessons Learned session
- Identifies any Process Improvements

3.1.2 Disaster Recovery Program Overview

The Disaster Recovery Program provides the direction needed to recover computer processing capabilities at an alternate processing site in order to maintain a viable BlueCross BlueShield of South Carolina (BlueCross) business organization.

In the event of a disaster that renders either the BlueCross or Companion Data Services, LLC, data centers unusable, procedures must exist to enable BlueCross to recover Infrastructure and Application Systems in order to continue processing. Critical production areas will be the first priority.

Disaster Recovery Plans (DR Plans) must be developed and maintained to document the recovery procedures for Application Systems and Infrastructure. Federal and State requirements, regulations, contractual agreements with customers, and testing requirements must be considered when developing a DR Plan. The DR Plan for each system must be reviewed by appropriate management and approved prior to its inclusion in the Disaster Recovery Program.

3.1.3 Disaster Recovery Program Onboarding

Production systems are required to be inducted into the Disaster Recovery Program (DR Program) to ensure that a plan is in place for recovering the critical production environment for business continuity. Whether or not there is a requirement to be included in Disaster Recovery Exercises, production systems must be included in the Disaster Recovery Program within 90 days of implementation into production.

A Disaster Recovery Plan is required for onboarding into the Disaster Recovery Program. This is typically the product of a work effort involving Recovery Management, ICT, and Tech Support (Refer to the section *Disaster Recovery Plans* below.). The area providing production support must approve the initial DR Plan. Refer to the section *Disaster Recovery Plans* below for instructions on adding a DR Plan to the DR Program.

NOTE For other references to Disaster Recovery Plans in the ISSM, refer to:

- *Technical Standards — Infrastructure > Overall Technical Infrastructure Standards > System Documentation Components > Technical Overview*
- *Technical Standards — Applications > Application Coding > Language Specific Standards > Non-Host Databases*

3.1.3.1 Disaster Recovery Exercise Onboarding

Disaster Recovery Exercises (DREs) are tests of the Disaster Recovery Program involving a limited portion of production, systems and data per the scope of the exercise, as defined by contractual obligations and sponsorship.

The following requirements are necessary for onboarding into a Disaster Recovery Exercise:

1. Completion of Disaster Recovery Program Onboarding more than six months prior to the DRE
2. A documented requirement for participation in the Disaster Recovery Exercise, which must be one or more of the following:

    a. Contractual requirements
    b. Customer-funded request
    c. I/S-approved request

When a requirement exists, the Disaster Recovery Plan Owner, System Owner, or requestor will notify the ICT PMO to include the system in the DRE. Initial participation of a system in a DRE is considered as a Proof of Concept (POC), where successful recovery of that system would be a secondary objective.

3.1.4 Disaster Recovery Plans

3.1.4.1 Maintenance of the Disaster Recovery Plan

The Disaster Recovery Program Office (DRPO) will ensure that DR Plans are updated and maintained in a location that provides sufficient access by the DR Plan Owners. Copies of the DR Plans are stored in the off-site tape vault.

The DR Plans must be reviewed and updated semiannually by the DR Plan Owners in accordance with government controls. The DR Plans will then be reviewed by the DRPO to ensure that the plans contain the necessary recovery information. In addition, I/S development project teams must review related DR Plans and ensure that appropriate changes are made to these plans due to enhancements, modifications, personnel, or other changes to the applications. Changes that impact Disaster Recovery Procedures must be reflected in the DR Plans.

Below is a list of other events that may require an update of the DR Plan:

- Transfer, promotion, resignation of critical personnel
- Significant modification of basic functions or data flow requirements
- Changes as a result of a risk assessment
- Changes in business operating environment
- Changes in communication network
- Changes in off-site storage facilities or methods
- Acquisition of new business
- New application platform development
- Retirement of an application system

3.1.4.2 Prioritization of the Recovery Process

Prioritization of application recovery (including application data) is established through an assessment by the Disaster Recovery Management Team once a disaster has been declared and the DR environment (infrastructure) has been established.

Key factors to consider when establishing recovery priorities include contractual obligations and operational impacts, such as for revenue-producing applications.

When prioritizing Application recovery activities, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are factors that must be considered.

Recovery Time Objective

The RTO focuses on how much downtime is acceptable and is the elapsed time between the system's failure and the system's reestablished availability at the alternate site. Production environments will be recovered first, followed by Development, Test, and other instances. The time to restore and recover the operations systems and databases may be 24 to 72 hours.

Business needs determine the choice of recovery technology. Global clustering, manual migration or tape restore are various options that are dependent on the acceptable timescales required to restore systems to a fully operational status.

The RTO must be stated clearly in terms of hours only.

Considerations in setting a system's RTO:

1. Determine how long user departments and/or customers can function without the system.
2. What is the contractual obligation?
3. Alternative processing (e.g., Alternative procedures will identify manual procedures that can be performed in lieu of system processing.).
4. Intersystem dependencies and their functions. (What systems must be available before an application can begin recovery?) The system's RTO will be in addition to the RTO of the other systems that it is dependent on.

Recovery Point Objective

The RPO determines the point in time to which data must be restored in order to resume processing.

The RPO must be stated clearly in terms of hours only.

If data is backed up once daily, the minimum RPO would be 24 hours. Any data entered in the time between the last backup and the disaster event would have to be re-entered.

Considerations in setting a system's RPO are:

1. Determine the system's absolute minimum restore point, which indicates how much data may be lost when recovering from a significant failure.
2. Determine if the system is critical to intersystem dependencies. (What systems rely on the availability of the application's data or processes in order to begin recovery?)
3. Can the processing of some input transactions be delayed?

3.1.4.3 Disaster Recovery Plan Requirements

When creating a new DR Plan, the DR Plan Owner will request a plan number from the Disaster Recovery Program Office (DRPO). The DRPO will assign a number and email the new DR Plan Template to the requestor. The DR Plan Template is the recommended content, which must be carefully considered to ensure effective and appropriate information is included in the DR Plan. Not all DR Plans have the same recovery processes and content; thus, not all components of the template will be used. All DR Plans must be written using instructions that are clear and can be followed by team members, externally contracted technicians or other IT professionals. The DRPO will provide the template upon request.

Recovery Management will consult with the Computer Operations, ICT and Telecom areas to ensure that any changes in capacity, equipment, or capability are properly reflected in recovery vendor contracts.

Disaster Recovery Plan Assertion

The purpose of a Disaster Recovery Plan is to document all the information necessary to recover a technology system in the event of a critical interruption or loss of a primary processing data center. The scope of information to be recorded is anything that would enable a qualified IT professional to recover the system to restore its compute service functions to business processes or other systems downstream. The objective is to recover all functionality critical for the continuity and recovery of the business within the shortest Maximum Tolerable Downtime (MTD) of a dependent business process. The strategy to accomplish the objective is to execute this plan within the RTO, assuming a total loss at the primary processing site and accessibility to only the data on recovery media stored from the last RPO.

DR Plan Owners

DR Plan Owners are responsible for ensuring that the plans cover the following activities:

- Identify essential missions and business functions and associated contingency requirements
- Provide recovery objectives, restoration priorities, and metrics
- Address contingency roles, responsibilities, assigned individuals with contact information
- Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure
- Address plans for necessary capacity for essential missions and business functions
- Plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustain that continuity until a full information system restoration
- Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented

DR Plan Owners are responsible for ensuring the following regarding their plans:

1. The DR Plan must be reviewed and updated:

   a. When changes are made to the system that affect the information in this plan.
   b. When a plan review cycle is initiated by the DRPO.

   The DR Plan Owner is responsible for notifying appropriate stakeholders of significant changes to the plan.

2. Persons, including managers and information systems users, must complete contingency training within 90 days of assuming an assigned role or responsibility in contingency, when necessary due to changes to the system, and every 365 days thereafter. DRPO manages an annual contingency training cycle, but the remainder of this requirement is the responsibility of the DR Plan Owner.
3. The DR Plan Owner is responsible for coordination with the organization responsible for the system in the development of the DR Plan.
4. The DR Plan Owner is responsible for ensuring that the plan accounts for the necessary capacity to provide for essential business functions.
5. The DR Plan must be suitable for the resumption of essential business functions within the business' MTD and the continuation of those functions until a full restoration to normal processing.

DR Plan Content

DR Plan Content must contain the following:

- System Properties
- Dependencies
- Recovery Team
- Workstation Requirements
- Data Requirements

System Properties

The system properties must include:

- DR Plan ID
- System Name, any aliases, and System Master Index (SMI) IDs
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- System Description
- Document Controllers (Owner, Coordinator, Support Coordinator, Technical Expert)
- Immediate Downstream Systems
- Immediate Downstream Business Processes

Dependencies

Understanding of system dependencies is imperative to ensure proper execution of a successful recovery. Dependencies must be documented to include:

- Immediate Upstream Systems
- Recovery Team
- Workstation Requirements
- Data Requirements
- Infrastructure Requirements
- Miscellaneous Requirements

Recovery Team

The Recovery Team is the group of persons required to execute this plan. The recovery participants who fulfill a Role listed in the DR Plan have a specific part to play in the recovery and may be from a system development area, support area, vendor company, or any other area. In the event of a Disaster or Exercise, the named members of the Recovery Team may be called upon to execute a recovery according to the procedures in this plan. The Roles (not job descriptions) are classified to help define the nature of a person's contributions toward the plan execution in the event the named members are unavailable, and alternates are assigned. Workstations and procedures are assigned to Roles.

Key information for each team member includes:

- Name
- Role (the role this person plays within the plan)
- Competencies (the skills and knowledge required for the role)

- Work Phone Number
- Alternate Number
- Email Address

Recovery Team members should have a basic understanding of the systems they would be required to recover. DR training is provided through periodic, mandatory review and understanding of DR Plans by participation in an actual Disaster Recovery Exercise (DRE) or both.

Vendor and other external contacts may be listed in this section if they have a role to play in the execution of the plan.

Workstation Requirements

The Recovery Team will need workstations to execute this plan. This section provides information about the workstations that would be needed. The workstations are classified with the Recovery Team Roles to help ensure that the person in that role has the tools to execute the process steps assigned to that role.

The necessary workstation requirements information includes:

- Role (the role within the plan this workstation is intended to support)
- Template/Archetype (the production workstation that can be used as a template)
- Domain & VLAN
- Software
- Firewall Rules
- Additional Requirements

Data Requirements

This section contains information about the critical data for the execution of this plan. The majority of the data is backed up through various means into media that is vaulted away from the primary processing site. The plan must record the production location of the data and the backup location, which is the initial location of the backup data known to the system owner.

Each System Owner is responsible for establishing appropriate tape vault patterns to rotate backup files from both data centers to the off-site vault. They must coordinate vault pattern updates with their System Support Team as appropriate.

Vital File Identifier Considerations

Vital File Identifier (VFI is the z/OS Disaster Recovery tool that monitors application cycles, identifies the critical files, generates recovery JCL and creates reports.

VFI Exclusions — VFI does not monitor Non-Host applications and databases. Non-Host areas and Database Administration are responsible for recovery of this data.

- The applications being monitored by VFI are not required to supply a list of datasets with their DR Plan; however, all Host DRPs should include the following verbiage: “VFI is used to monitor and recover this application.” The DR Plan must list the VFI libraries that are used to monitor and recover their applications.

VFI Availability

Access to VFI is obtained by requesting permission from the VFI Administrator.

Application owners are responsible to ensure that all critical datasets required to recover their applications are backed up and vaulted. To change or update data in a VFI application, they must submit a Service Request using the IT Business Systems Help form. They must also coordinate VFI changes with their System Support Team as appropriate.

Infrastructure Requirements

This is not an exhaustive list of the physical and virtual infrastructure required to execute this plan as it assumes the additional infrastructure is in place for the dependent systems upstream. The upstream systems are listed in the System section of the plan.

Host-Only systems need only list the Mainframe for Infrastructure Requirements, but all systems with Non-Host infrastructure must list the information necessary to restore these dependencies.

Disaster Recovery Procedures

The procedures in this section of the DR Plan are to recover the system in an actual disaster. The procedures and steps are planned and tracked with the procedures table and reference detailed procedural information in the plan document. Procedures should be broken out by sessions of uninterrupted steps so overall planning and allocation of resources can be optimized for the recovery as a whole.

Disaster Recovery Exercise Procedures

The procedures in this section of the DR Plan are to recover the system in a Disaster Recovery Exercise. The procedures and steps are planned with the procedures table and reference detailed procedural information in the plan document. Procedures should be broken out by sessions of uninterrupted steps so overall planning and allocation of resources can be optimized for the exercise as a whole.

Disaster Recovery Exercise Procedures sections must also include a statement describing how the exercise procedures demonstrate preparedness of the recovery solution for an actual disaster.

Document History

Each Disaster Recovery Plan must include a three-year history of changes and reviews for the document. The Document History table shall include the date, responsible person, and a description of any changes.

3.1.4.4 Disaster Recovery Plan Cloud Services Components

All systems that include a cloud service as part of its Disaster Recovery Plan must also include continuity components for the service in their plan.

In addition to the procedure playbooks describing BlueCross procedures for a Disaster Recovery and Disaster Recover Exercise, the plan must include playbooks for scenarios where there is a disaster, outage, or impairment on the end of the cloud service.

Appendix Items that must be included for each cloud service if applicable:

- Provider's general DR or continuity plan (including their RPOs and RTOs) reviewed within the last year
- Evidence of the provider's last DR Exercise, or test of the provider's continuity
- Provider's outage statistics report
- Provider alternatives that were evaluated
- Information that would be needed if the provider were replaced with another

3.1.4.5 Disaster Recovery Plan Update Procedures

The Disaster Recovery Plan provides information necessary to recover mission critical I/S processes and applications. DR Plans will be inventoried in the ***SharePoint Online (SPO)*** system by the Disaster Recovery Program Office (DRPO). Copies of these plans have been placed in the BlueCross BlueShield of South Carolina Vault.

DR Plans are typically updated, as applicable, as part of the normal Systems Work Request Methodology. However, a formal DR Plan review and update occurs semiannually by the DR Plan Owners in accordance with government controls and the DRPO.

Reviewing or Updating an Existing DR Plan

To review or update an existing DR Plan follow these steps:

The DR Plan Owner will:

1. Review the procedures for updating the DR Plan.
2. Access the DR Plan in the ***SPO*** library using the following URL: https://bluesc.sharepoint.com/sites/disrecpln/_layouts/15/viewlsts.aspx?BaseType=1&view=14.
3. Update the DR Plan using Microsoft Word.
4. Notify DRPO via email when the plan has been updated.

The DRPO will:

1. Review the DR Plan and accept or provide suggested changes.
2. Publish the major version of the plan in ***SPO***, once the DR Plan is deemed to be complete.
3. Update the DR Plan Tracking Worksheet.
4. Place a copy of the DR Plan in the vault.
5. Keep management notified of the DR Plan update progress.

During the review process, the following sections will be verified:

- Change/Review History (Date Updated, Reviewer Name, Action Taken)
- Application or System Description
- Section I — Recovery Team Contact Information (Name, Department, Phone Numbers, etc.)
- Section II — Dependencies (Support systems, shared databases and/or libraries, etc.)
- Section III — Data Considerations (Recovery tool files, RPO, RTO, etc.)
- Section IV — Recovery Procedures (Detailed steps, actions, notes, etc.)
- Section V — DR Exercise Procedures (Exercise specific information, actions, notes, etc.)
- Section VI — Appendices
    - Appendix A — Internal Notification Contacts

  - Appendix B — Vendor Contacts
  - Appendix C — Other External Notification Contacts

- Overall Review

  - Any files required for VFI recovery are vaulted in an off-site vault.
  - The DR Plan is written for a real disaster.
  - DRE specific instructions are listed in Section V of the DR Plan.

The DR Plan Owners are responsible for the content and semiannual review of their DR Plans.
The DR Plans must be maintained according to current Disaster Recovery and operating standards.

Adding a New Plan

New DR Plans are typically written as part of a Work Request that implements new Applications or Infrastructure.

The creation of a new DR Plan is a critical part of the DRE Onboarding Process.

The following is the process for adding a new plan:

1. Requester will send an email to DRPO to request a DR Plan template.
2. DRPO will assign a plan number to the template and forward the template to the requestor by email.
3. Requester will create the plan using the template provided by DRPO.
4. When all DR Plan updates have been made by the DR Plan Owner, they will forward the plan to their area's approver.
5. Approver will review the plan updates/changes.
6. Once approved, approver will email the updated plan to the DRPO at email address DRPO.
7. DRPO adds the plan to the DR Plan Inventory and loads the new plan to ***SPO***.

Retiring an Existing Plan

To retire an existing DR Plan, follow these steps:

1. Send an email to DRPO to request that the DR Plan be retired. A business reason for retiring the DR Plan should be included with this request.
2. DRPO will move the DR Plan into the respective Retired folder in ***SPO***.
3. DRPO will rename the DR Plan by placing "RETIRED" at the beginning of the DR Plan Name.
4. DRPO will remove the DR Plan from the DR Plan Inventory List.

3.1.5 Disaster Recovery Exercise Overview

The purpose of performing the Disaster Recovery Exercise (DRE) is for the customers and company to attain a ***reasonable business assurance*** that systems and infrastructure that are required to execute critical business functions can be recovered at the designated recovery site within the stated Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Verification that the recovery has been successfully completed is attained by the testing of pre-determined systems. By processing a sampling of data through standard work processes and verifying the result, business units and customers can attain a reasonable business assurance that all supporting systems and infrastructure have been successfully

reconstituted. This is evidenced by a completed Customer Sign-off form for the customer-facing systems exercised.

The DRE will be conducted at a vendor provided hot site every 365 days. Date exceptions can be applied in the event that the DRE falls on a federally observed holiday or if a true disaster occurs. If one of the exception elements occurs, the DRE can shift 10–15 days prior to or after the start of the next 365-day cycle to accommodate scheduling impacts to the calendar. Each system area will have input into the financial decision for identifying systems that will be included in the annual DRE.

The annual DRE will be run using the procedures in the official DR Plan document stored in a secure location by the Disaster Recovery Program Office. This will evaluate the effectiveness of the documented DR Plan.

For instructions on participating in a DRE for the first time, please refer to the section *Disaster Recovery Exercise Onboarding* above.

There are several reasons for running periodic DREs. The DRE:

- Complies with legal, contractual, and regulatory requirements.
- Proves that the plan works and can meet the business recovery requirements.
- Proves that the plan has been properly updated.
- Proves that backed-up data is adequate to support recovery of specified business functions.
- Provides staff member training.
- Raises general awareness.

3.1.5.1 DRE Activities

DRE Planning

Each DRE is scheduled several months in advance by the Recovery Management team working with the Recovery Vendors. Dates are presented as tentative until a test proposal is received and verified.

A work effort is created to allow staff members to be assigned to participate in a given DRE, in addition to their other assignments. A DRE Program Lead will coordinate meetings and communication with LOB Project Managers, including the ICT Project Manager, for all Infrastructure activities.

Major milestones for DRE planning include the following:

- Finalize the scope of the DRE (e.g., which applications and functions will be included).
- Define the Recovery Infrastructure requirements.
    - LOB Application Owners work with Recovery Management and ICT to assure resources are available at recovery sites.
    - The Recovery Vendor and Application Owners finalize plans, which are also reviewed for accuracy.
- Review/finalize workstation, printer and phone requirements and seating chart (if applicable) for the recovery site to be used in the exercise.
- Develop a task time line to be used during the exercise.
- Review/finalize communication plans and contact lists, to support a 24x7 exercise (e.g., shift schedules, on-call schedules, etc.).

Test Plans

A DRE Test Plan form will be submitted by the I/S area recovering the system or application to their assigned Project Management Office (PMO), if applicable, and Recovery Management prior to a scheduled DRE. This form will typically request the following information:

1. The system or application that will be recovered (e.g., AMMS, MEMB, CSR Desktop, etc.)
2. The portion of the system that will be recovered (e.g., entry, adjudication, enrollment)
3. The test objective (e.g., Restore desktop for customer interfacing)
4. How the test objectives will be verified (e.g., customer verification, Systems Support Group [SSG] verification, etc.)
5. If Customers will participate in the DRE and, if so:
   a. The person responsible for customer sign-off documentation
   b. A test matrix, if applicable
6. A summary of the overall expected results of the recovered system

Each system or application owner (Enterprise Server areas only) will be responsible for supplying the appropriate schedules to recover and run batch cycles through the automated scheduler. ZEKE or Tivoli DRE schedules must be sent via email to the appropriate scheduling account no later than two weeks prior to the DRE Declaration Date.

Each system or application owner will be responsible for contacting the appropriate software vendors and informing them that BlueCross is performing a DRE and that their software is running on a backup site, if applicable. If this is unique to the application, it must be a part of the contract terms with the vendor.

DRE Execution

The DRE Program Lead communicates to DRE participants and management the declare date for the DRE, when the exercise has started and finished, and when various milestones have occurred.

In addition, regularly scheduled communications are provided around the clock throughout the 24x7 exercise to all DRE participants and various levels of management by the DRE Program Lead and LOB Project Managers (LOB PM).

Each LOB PM is responsible for assuring that all DRE validation (e.g., recovery validation) is documented in at least two formats, to assure redundancy in case something happens to one format, and is responsible for assuring that there is sign-off for each application that was tested during the DRE.

Each LOB PM and/or system or application owner is also responsible for documenting problems encountered during the planning and execution phases, including those that occur while reconstructing files and running batch cycles.

Issues or problems that occur before and during the DRE will be submitted to the email address *Lessons_Learned* for review and follow-up.

Once all Lessons Learned have been collected, the DRPO develops an Executive Summary overview report of the exercise.

Sign-off Forms

At the conclusion of the DRE, a completed Customer Sign-off form will be included in the post-test documentation for each customer-tested application. A standardized sign-off form is provided by the DRE Program Lead or LOB Project Managers.

A completed DRE Customer Sign-off form must include:

- The customer name.
- The customer area.
- The name of the system or application the customer tested during the DRE. (If the name is unknown to the customer, the assigned I/S Project Manager should assist in providing this information.)
- The signature of the customer. (This customer sign-off will typically be a representative of a business unit [e.g., TRICARE Claims, Major Group Commercial Membership, etc.] but can be an I/S staff member when the testing is internal to an I/S area and/or the customer is actually an I/S staff member.)
- The date of the sign-off.

The timely resolution of issues and customer comments written on the DRE Customer Sign-off form are the responsibility of the application teams.

3.1.5.2 Post-Exercise DRE Activities

The DR Plan may be updated as needed by the system or application owner after the conclusion of the Disaster Recovery Exercise for changes to existing procedures to resolve problems encountered during the Disaster Recovery Exercise.

The system or application owner is responsible for obtaining output from the last current production cycle sufficient to verify the results and balance the Disaster Recovery Exercise.

Each I/S area participating in the Disaster Recovery Exercise should submit a *Test Results Form* to the DRE Program Lead or respective LOB Project Manager following the completion of the DRE.

When Corporate Audit selects an application for auditing immediately following the DRE, managers of the responsible I/S areas will report DRE results (per the Audit document request list) to their assigned PMOs (if applicable), and to the Disaster Recovery Program Office (DRPO).

The DRE Audit may include, but is not limited to the following:

- The Disaster Recovery Exercise test results document (must be submitted in soft copy)
- Where applicable, Customer Test Matrices used to test system functions
- Where applicable, screen prints to verify results
- Where applicable, an *I/S* or *Customer Sign-off* form for the application validated. A completed *Customer Sign-off* form must be submitted in soft copy and will include:

    - The customer name.
    - The customer area.
    - The name of the system or application tested.
    - The signature of the Customer and/or I/S representative.
    - The date of the sign-off.

3.1.5.3 Lessons Learned

All areas are encouraged to participate in the Lessons Learned session. It is understood that not all areas will experience issues during the DRE.

Issues or successes may be submitted to the email address *Lessons_Learned* at any time during the pre-DRE phase, the actual DRE, or the post-DRE phase.

During the two weeks following the DRE, the means of gathering the issues or process improvements will be by email to *Lessons_Learned* with copies going to the DRE Program Lead and all appropriate Project Managers.

If work sessions are needed to collect issues, the Project Managers will conduct those sessions with their application areas or customers during this same two-week period. Best efforts should be made to resolve issues within an application or customer area during this time.

The DRE Team works with the team responsible for the Lessons Learned session to ensure that each Lessons Learned is correctly categorized (i.e., Lesson Learned, Defect, and Process Improvement) and, if applicable, to assign an Action Plan owner to address the lesson learned.

DRPO then includes a *Lessons Learned Summary* in the overall DRE Executive Summary. Issues are tracked to resolution by the ICT Project Management Office (PMO). Each Lessons Learned Action Plan is expected to be completed by the Action Plan owner prior to the next DRE.

3.1.6 Business Continuity

The Business Continuity Group (BCG) assists Customers by coordinating periodic mandatory Business Continuity (BC) Plan updates. Recovery Management assists the BCG with all I/S Business Life Safety Plans.

Business Continuity I/S Life Safety Plans are location specific and include detailed information regarding Evacuation Teams, employee contact numbers, and evacuation details.

Business Continuity Life Safety Plans contain a listing of Evacuation Teams that are defined for each Building/Department. Floor Wardens are assigned to monitor and assist each Department in each Building.

The Business Continuity I/S Life Safety Plans are stored in the Assurance CM Software Tool, where they are reviewed and updated during each mandatory review cycle and posted on the I/S Portal for review and print.

Business Continuity I/S Life Safety Plans are made available for viewing via the I/S Portal. Go to My e-Work > I/S Portal > Reference Library > Business Continuity and select the provided link. The link opens in SharePoint to Disaster Recovery Plans > Business Continuity > All Documents.

3.1.6.1 Business Continuity Plan Update Procedure

The BCG manages BC Plans for the various Business Units in order to continue or resume services in the event of a disaster.

The Disaster Recovery Program is a subset of Business Continuity and is specific to compute services.

The BCG interacts with I/S via the Disaster Recovery Program Office (DRPO) to maintain the BC Plans and to communicate business needs during a true Disaster Recovery, or whenever the Corporate Emergency Response Team (CERT) is in session.

3.1.6.2 Floor Warden Responsibilities

Floor Wardens are responsible for ensuring that all employees safely evacuate the building in the event of an emergency. The target is two Floor Wardens per 20 employees — a primary and a secondary. Floor Wardens are chosen by managers and are required to complete annual Floor Warden training.

NOTE Contact BC.ADMIN for the Corporate Safety Administrator class schedule.

Floor Warden training is an annual requirement that is facilitated by the Corporate Safety Administrator. In addition to the annual training, Recovery Management, at the request of the assigned Floor Wardens, will conduct and facilitate additional training session where they will conduct a functional a walkthrough of the area to simulate an evacuation. To schedule a departmental walkthrough, make updates to Floor Warden assignments, or to find out when annual Floor Warden training is being held, contact **BC.ADMIN**.

3.1.6.3 Business Continuity Exercises

A Business Continuity Exercise (BCE) is conducted each year to test the Business Continuity Plans.

BCEs are conducted to ensure that the company can recover business functions at an alternate work facility in the requested timeframes. Business Continuity Exercises are conducted at an alternate site, such as the NetBank building,

These Exercises are conducted using Production Infrastructure, Telephony, Applications, Networks and Databases.

During the Business Continuity Exercise, it is expected that required Production system components work properly during customer testing.