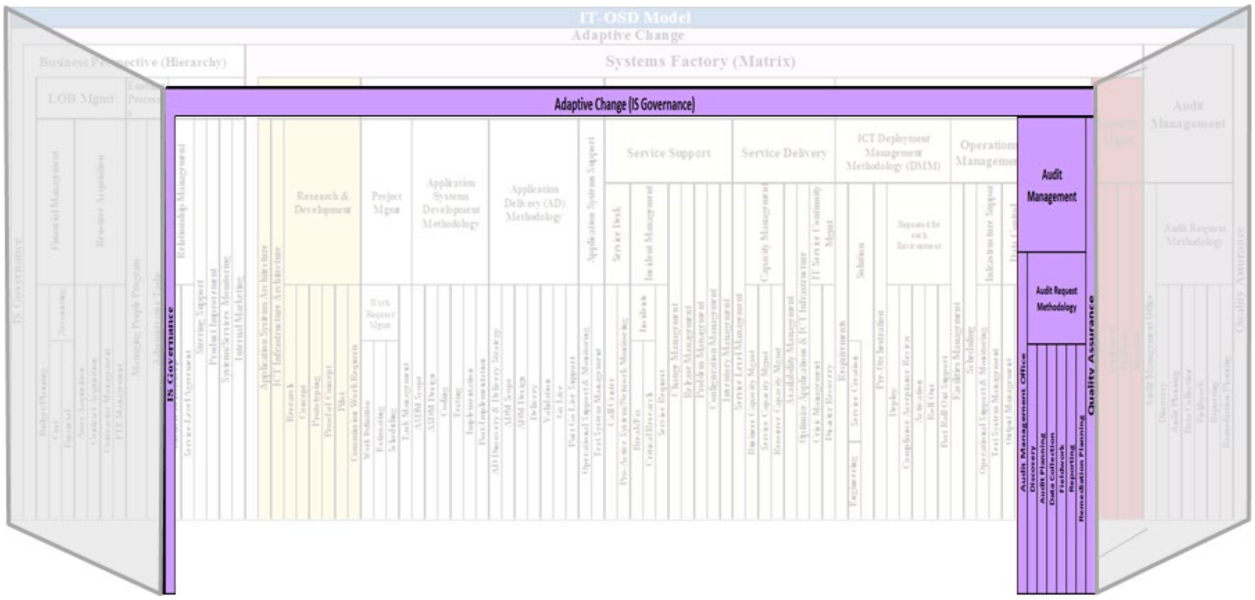
South Carolina

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

imagination to Implementation
INFORMATION TECHNOLOGY

Adaptive Change



Information Systems Standards Manual

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

Table of Contents

Table of Figures

List of Tables

Chapter 1 Adaptive Change and I/S Governance

1.1 I/S Governance Committee Structure

1.1.1 I/S Governance Committee Structure (Detailed View)

Chapter 2 Information Systems Policy Committee

2.1 Responsibilities

2.2 ISPC Subcommittees

2.3 Management Practices Manual

Chapter 3 Information Systems Standards Committee

3.1 Description

3.2 Voting Membership

3.3 ISSC Work Groups: Subcommittees, User Groups and Task Forces

3.3.1 ISSC Work Group Chair Responsibilities

3.3.2 Standing ISSC Work Groups

3.4 I/S Lighthouse

3.4.1 Access

3.4.2 Content Management Access

3.4.3 Responsibilities

3.4.4 I/S Lighthouse Content

3.4.5 Content Review

Chapter 4 The Information Systems Standards Manual

4.1 ISSM Maintenance

4.1.1 ISSM Numbering and Reference Formatting

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

4.1.2 ISSM Annual Review

4.1.3 Recommendations from the Work Groups to the ISSC

4.1.4 Proposed Changes to the ISSM

4.1.5 Cosmetic Changes

Chapter 5 Process Audit

5.1 Waivers

5.2 Standards Review

Chapter 6 Global Standards

6.1 Reviews

6.1.1 Periodic Reviews

6.1.2 Architectural Reviews

6.2 Methodology Documentation — Overview

6.2.1 Documentation Confidentiality Disclaimer

Chapter 7 Standards for Non-I/S Areas

7.1 Software Development/Maintenance Responsibilities

7.1.1 Administration

7.2 End-User Computing

7.2.1 End-User Supported Software

7.2.2 End-User Supported Software Procurement

Chapter 8 Audit Management

8.1 Overview of the Audit Management Office

8.2 Audit Request Management

8.2.1 Ongoing Life Cycle Requirements

8.2.2 Steering Support Process

8.2.3 Audit Request Management Processes

8.3 Audit Request Methodology

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

8.3.1 Purpose of Audit Request Methodology

8.3.2 Audit Role

8.3.3 Audit Request Methodology Phases

8.3.4 Audit Planning Phase

8.3.5 Data Collection Phase

8.3.6 Fieldwork Phase

8.3.7 Reporting Phase

8.3.8 Remediation Planning Phase

8.3.9 Closure

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

Table of Figures

Figure 1-1 I/S Governance Committee Structure

Figure 1-2 I/S Governance Committee Structure (Detailed View)

Figure 8-1 Audit Request Life Cycle

Figure 8-2 Audit Accountability Matrix

Figure 8-3 Discovery Phase

Figure 8-4 Audit Planning Phase

Figure 8-5 Data Collection Phase

Figure 8-6 Fieldwork Phase

Figure 8-7 Reporting Phase

Figure 8-8 Remediation Planning Phase

List of Tables

Table 3-1 Standing ISSC Work Groups

Table 3-2 I/S Lighthouse Content Ownership

Table 4-1 ISSM Text Reference Format

Table 4-2 ISSM Content Review

Table 8-1 Audit Request Methodology Summary Matrix

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

Chapter 1 Adaptive Change and I/S Governance

Adaptive Change requires an IT organization to recognize the need or opportunity to adapt and then to apply an analytical and systematic approach to making the necessary adaptations. There are two basic components of the analytical and systematic approach: an IT governance system and an IT quality assurance system.

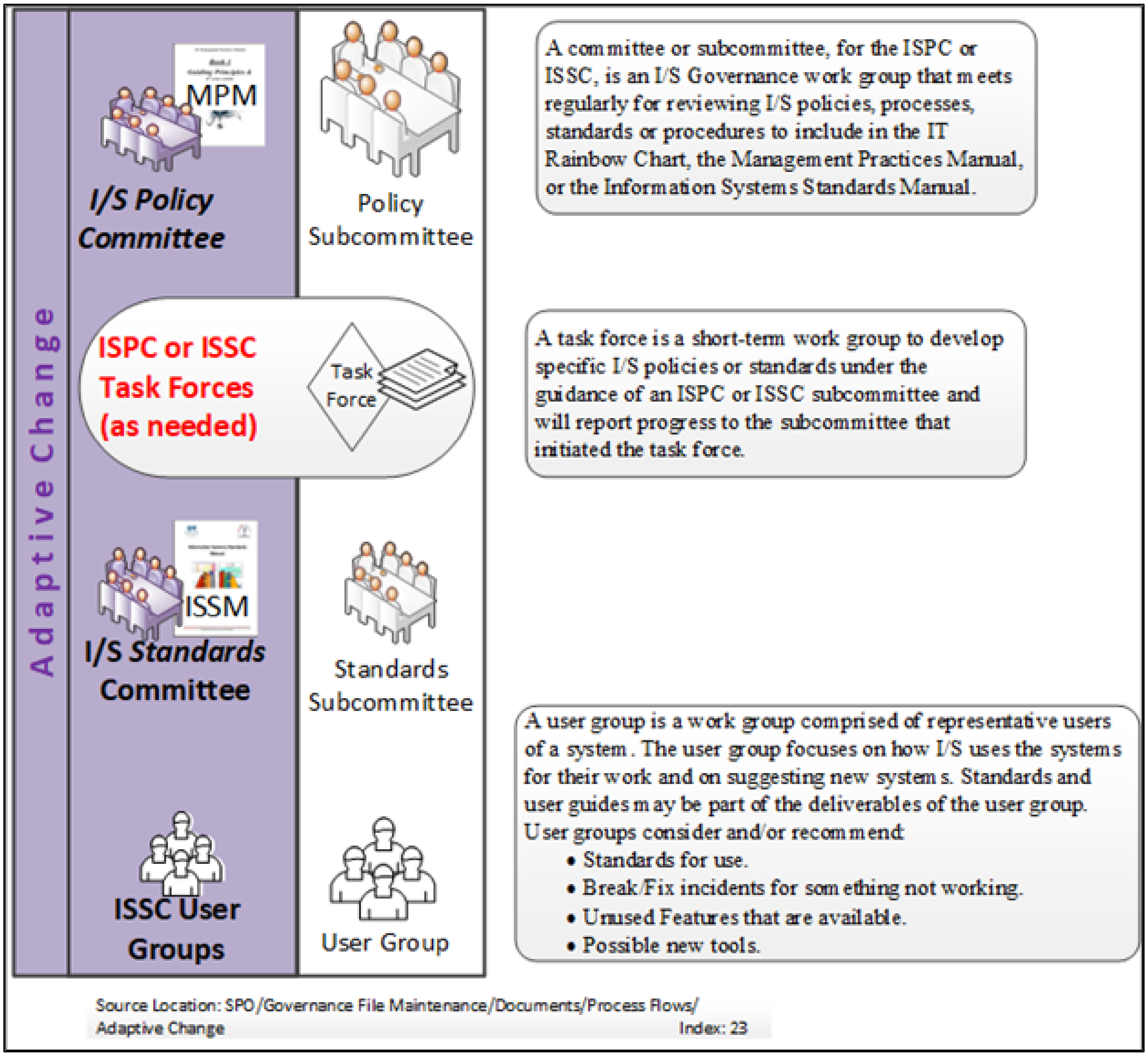
The Adaptive Change process allows for innovation and adaptation within an organization's administrative and operational areas. Change is more easily adapted by establishing a governance process over both technical and management policy and practice. The Information Systems (I/S) Governance process consists of persons comprising committees who make up a governing body for the purpose of authorizing technical and management standards and practices documented within I/S Governance manuals. These committees are described below:

- The **Information Systems Policy Committee (ISPC)** has the oversight responsibility for management policy and practice by the I/S Hierarchy.
- The **Information Systems Standards Committee (ISSC)** has the oversight responsibility for technical policy, process, and practice by the I/S Matrix.

A process audit complements IT governance by providing both comparative measurements and other data to assist the governance process in evaluating the effectiveness of the I/S Matrix processes. It employs audit and investigative processes to examine, evaluate, and analyze internal controls, processes, and management procedures utilized in the I/S Hierarchy to ensure that they are working effectively to improve the overall efficiency and general health of the IT staff and system resources.

1.1 I/S Governance Committee Structure

The I/S Governance Committee Structure is composed of the ISPC and its policy subcommittees, the ISSC and its standards subcommittees, user groups and task forces. This is shown in Figure 1-1.



A committee or subcommittee, for the ISPC or ISSC, is an I/S Governance work group that meets regularly for reviewing I/S policies, processes, standards or procedures to include in the IT Rainbow Chart, the Management Practices Manual, or the Information Systems Standards Manual.

A task force is a short-term work group to develop specific I/S policies or standards under the guidance of an ISPC or ISSC subcommittee and will report progress to the subcommittee that initiated the task force.

A user group is a work group comprised of representative users of a system. The user group focuses on how I/S uses the systems for their work and on suggesting new systems. Standards and user guides may be part of the deliverables of the user group. User groups consider and/or recommend:

- Standards for use.
- Break/Fix incidents for something not working.
- Unused Features that are available.
- Possible new tools.

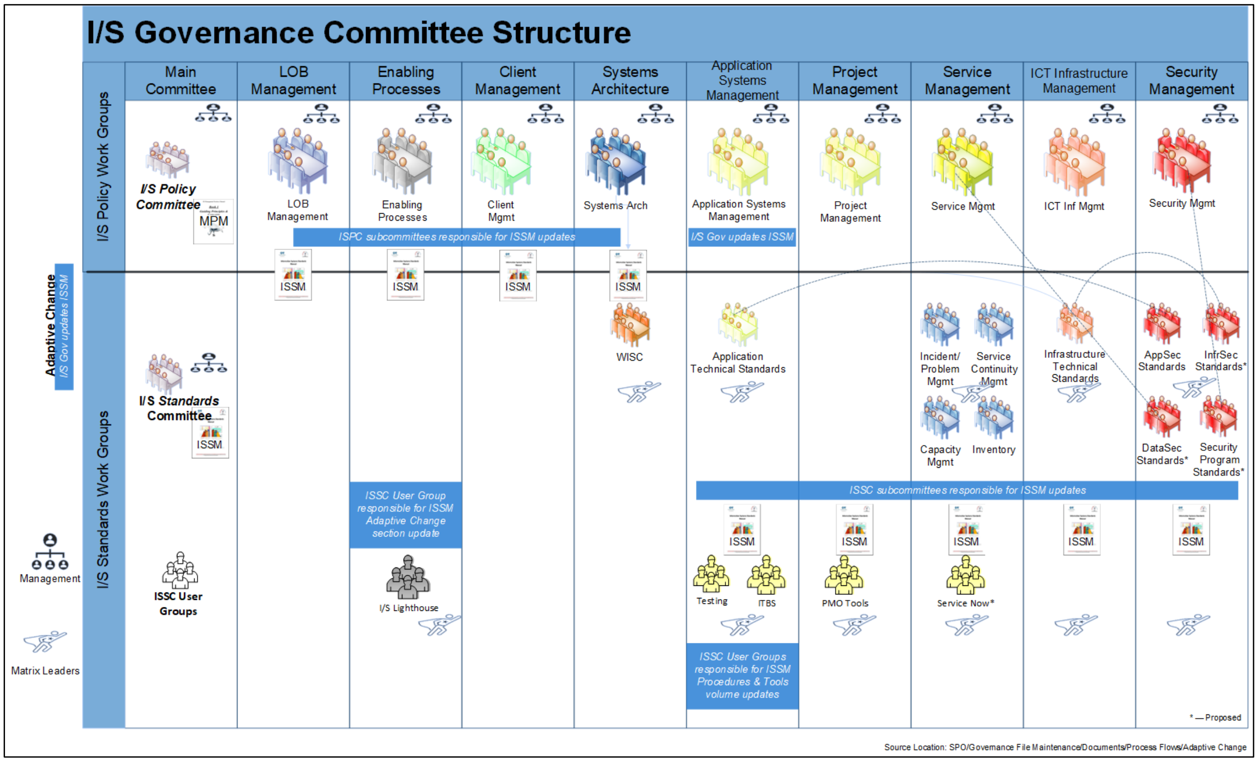
Source Location: SPO/Governance File Maintenance/Documents/Process Flows/
Adaptive Change Index: 23

Figure 1-1 I/S Governance Committee Structure

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

1.1.1 I/S Governance Committee Structure (Detailed View)

Below is a detailed view (Figure 1-2) of the I/S Governance committee structure illustrating how the ISSC and ISPC work groups interact.



Source Location: SPO/Governance File Maintenance/Documents/Process Flows/Adaptive Change

Figure 1-2 I/S Governance Committee Structure (Detailed View)

NOTE See the I/S Lighthouse for the full committee structure as well as the current committee chairs.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

Chapter 2 Information Systems Policy Committee

The **Information Systems Policy Committee (ISPC)** is made up of experienced management representatives from all functional areas within the organization.

The ISPC and its subcommittees and task forces work with the Information Systems Standards Committee (ISSC) and its ISSC work groups to ensure that appropriate management controls are put in place around all highly repeatable processes.

2.1 Responsibilities

The ISPC and its standing subcommittees are responsible for the contents of the I/S Management Practices Manual (MPM) and provide management guidance to the ISSC.

2.2 ISPC Subcommittees

There is an ISPC subcommittee for each of the nine major processes in the IT Rainbow Chart. The Application Systems Management process has one additional subcommittee, the ISPC Project Management Subcommittee.

The ISPC serves as the Adaptive Change policy subcommittee. The ISPC subcommittees are listed below:

- Application Systems Management
- Client Management
- Enabling Processes
- ICT Infrastructure Management
- LOB Management
- Project Management
- Security Management
- Service Management
- Systems Architecture

The I/S Governor is the chair of the ISPC. The chairs for the subcommittees are listed in the I/S Lighthouse.

2.3 Management Practices Manual

The I/S MPM captures the essence of what and why we do what we do in the manner in which we do it to be successful. The factors that have resulted in our success have evolved over time. I/S Senior Management has either fully embraced or adapted to proven concepts and techniques, and incorporated guiding principles to support a model that considers how processes and resources should be integrated and aligned to produce a desired outcome.

The ISPC subcommittees or the ISPC itself, as assigned by the ISPC Chair, will review the MPM sections when deemed necessary. The completion of each review will be recorded in the ISPC meeting minutes. The I/S MPM is both a strategic and day-to-day operational guide. A thorough review is best done in conjunction with available training classes and materials related to I/S Management and leadership.

Chapter 3 Information Systems Standards Committee

3.1 Description

The **Information Systems Standards Committee (ISSC)** is made up of representatives from all functional areas within the Information Systems (I/S) organization. A designee of the I/S Governor is the chair of the ISSC.

The ISSC has the following functions:

- The ISSC and its work groups own the contents of the ISSM.
- The ISSC works with the I/S Policy Committee to ensure that appropriate management controls are put in place around all highly repeatable processes.
- The ISSC provides a forum for Information Systems staff to submit questions or concerns about their programming environment or methodology, to request clarification of formats or guidelines, to identify process improvement opportunities, or to ask other questions. Not every issue, however, that is presented to the ISSC results in a new or modified standard.

The ISSC meets once every month. The ISSC Chair or designee may call special meetings outside of the regular monthly meetings to discuss a specific topic.

Minutes from each ISSC meeting are documented and distributed as described below:

1. The minutes of each ISSC meeting will be documented, stored in ***SharePoint Online (SPO)*** and distributed to the ISSC members.
2. The attendance record will be recorded in the meeting minutes.
3. An archive history of meeting minutes will be retained for no less than five years.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

3.2 Voting Membership

The ISSC and its work groups own the contents of the ISSM. Proposed changes to the ISSM are classified as either votable or non-votable. For details on the proposal process, refer to *Adaptive Change > The Information Systems Standards Manual > ISSM Maintenance > Proposed Changes to the ISSM.* The representative areas shown below are the voters for those standards requiring a vote. Voting members of the ISSC are from the I/S Hierarchy. Voting members are also tasked with keeping their respective areas informed of ISSC activities and proposed and approved changes.

- Acquisition and Inventory Management Services
- CDS
- CGS
- Commercial Application Systems
- Commercial PMO
- Compliance Oversight and Risk Reporting
- Cyber Threat Intelligence
- Data Security
- Data/Voice/Network
- Database Administration
- Digital Leveraged Systems
- EDI Gateway Host
- EDI Gateway Non-Host
- End User Services
- Enterprise Architecture
- G&A
- Governance
- ICT Client, PMO and Reporting
- ICT Delivery Services
- ICT Distributed Data Center
- ICT Mainframe
- ICT Risk & Compliance
- Palmetto GBA Medicare
- PGBA Applications
- PGBA Client
- PGBA/Medicare PMO
- PGBA Quality
- PMO & Testing
- Service Management
- Staff Resource Management
- Systems Support
- TSC Service Desk
- Workstation Support

3.3 ISSC Work Groups: Subcommittees, User Groups and Task Forces

The ISSC Chair may charter work groups called **subcommittees**, **user groups** and **task forces** as needed to focus on specific sections of the ISSM. Members of these ISSC work groups come from the areas affected by the standards the ISSC work group is responsible for. At least one member of the work group should be a voting member of the ISSC. The ISSC work groups address any standards and processes for accomplishing the work and services provided by the Information Systems Division as described by the IT Rainbow Chart. These work groups are responsible for conducting the annual review of the ISSM chapters as applicable. For details on the annual review, refer to the section *Content Review* later in this chapter.

Subcommittee — An ISSC-chartered work group that meets regularly for reviewing I/S processes, standards or procedures to include in the ISSM. The proposed changes may also affect the MPM.

User Group — An ISSC-chartered work group comprised primarily of representative users of a system or group of systems. A user group focuses on how I/S uses the systems for their work and on suggesting new systems. Standards and User Guides may be part of the deliverables of the user group. User groups consider or recommend:

- Standards for use.
- Break/Fix incidents for something not working.
- Unused features that are available in an existing system.
- Investigating new tools.

Task Force — An ISSC-chartered, short-term work group to develop specific I/S policies or standards under the guidance of an ISSC subcommittee and will report progress to the subcommittee that initiated the task force. Task forces initiated by the ISSC will be added to the ISSC's monthly agenda to report on progress.

3.3.1 ISSC Work Group Chair Responsibilities

Each ISSC work group must have a chair that is approved by the ISSC Chair. The chair of the work group has the responsibility to see that the following standards are met:

- All work group meetings must be held on a regularly scheduled basis, which can vary from monthly to quarterly depending on the purpose of the work group.
- All documentation created by a work group must be stored and published in the work group's assigned ***SPO*** governance site.
- An agenda should be published prior to the scheduled meeting.
- Minutes must be taken at all work group meetings and published to the work group members as well as to the ISSC and, if requested, to Sr. Management.
- The minutes should include the date, time and location of the next meeting, if available.
- The work group chair should track action items between meetings to ensure that activity is occurring.
- The work group chair must attend the monthly ISSC meeting and give a status report of the work group's activities.

- Requests for changes to a work group (e.g., chair, name, or responsibilities) should be sent to the ISSC Administrator for review with the ISSC Chair for approval.

NOTE Anyone needing access to an ***SPO*** site for the ISSC or the ISPC can send an e-mail to IS-QA-PROCESS-MGMT.

3.3.2 Standing ISSC Work Groups

The purpose of this table is to identify those work groups that the ISSC has approved as long-term or standing subcommittees (Table 3-1). These are expected to exist until the ISSC deems their use unnecessary.

Standing ISSC Work Groups

ISSC Work Group	Responsibilities
Application Security Standards Subcommittee	Establish the standards that apply to the security of our internally developed applications.
Application Technical Standards Subcommittee	Establish and oversee standards that apply to application systems software development.
Capacity Management Subcommittee	Establish and oversee 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.
Data Security Standards (Proposed)	TBD
I/S Lighthouse User Group	Establish and oversee the guidelines and standards that apply to the I/S Lighthouse. This user group will also review and approve requests for enhancement and expansion of the existing I/S Lighthouse framework.
Incident/Problem Management Subcommittee	Establish and oversee 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.
Infrastructure Security Standards (Proposed)	TBD

Standing ISSC Work Groups

ISSC Work Group	Responsibilities
Infrastructure Technical Standards Subcommittee	Establish and oversee the standards that apply to the infrastructure. These standards will address all relevant issues regarding hardware, software, middleware and operational topics.
Inventory Subcommittee	Evaluate, justify and prioritize any proposed enhancement or activities that deal with the systems for procurement, contracts and the management of assets. This subcommittee will, in addition, oversee and monitor related standards.
IT Business Systems (ITBS) User Group	Evaluate, justify and prioritize any proposed enhancement or activity that deals with systems used by the I/S staff, except those ITBS covered by other user groups. In addition, oversee the related standards.
Project Management Office (PMO) Tools User Group	Establish and oversee the systems that facilitate project management processes and tools used by the project management areas.
Security Program Standards (Proposed)	TBD
Service Continuity Management Subcommittee	Establish and oversee the guidelines and standards that apply to the work done by I/S for Crisis Management and Disaster Recovery.
Service Now User Group (Proposed)	TBD
Testing User Group	Evaluate, justify and prioritize any proposed enhancement or activities that deal with testing tools (e.g., Quality Center) and development regions or testing regions. They will, in addition, oversee and monitor testing-related standards.
Workstation Infrastructure Subcommittee (WISC)	Establish and oversee the standards that apply to the workstation infrastructure. These standards will address all relevant workstation issues regarding hardware, software and operational topics.

Table 3-1 Standing ISSC Work Groups

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

3.4 I/S Lighthouse

The Information Systems (I/S) Lighthouse is a SharePoint Online tool and is the standard method used to provide the I/S staff with effective access to information pertaining to how to do their job and the tools they use to perform their job responsibilities. It is located under the existing My e-Work intranet site. The I/S Lighthouse pulls together existing documentation used in various I/S departments and allows for organized, easy access while managing the content for this documentation.

3.4.1 Access

View access to the I/S Lighthouse is automatically granted to all I/S employees and contractors. The Active Directory groups controlling access to the site are owned by the Process Audit department.

Non-I/S staff may request view access using the Network Access - Add/Change/Delete form and request to be added to the ISP_MANAGER_ACCESS_NON-IS active directory group.

3.4.2 Content Management Access

The I/S Lighthouse content is owned by our I/S Policy Committee (ISPC) subcommittees and is aligned to I/S Processes (Table 3-2).

I/S Lighthouse Content Ownership

I/S Process	Responsible ISPC Subcommittee
Application Systems Management	Application Systems Management
Client Management	Client Management
Employee Hub	Enabling Processes
ICT Infrastructure	ICT Infrastructure Management
LOB Management	LOB Management
Manager Hub	Enabling Processes
News & Events	Enabling Processes
Project Management Office	Project Management
Security Management	Security Management
Service Management	Service Management
Systems Architecture	Systems Architecture

Table 3-2 I/S Lighthouse Content Ownership

3.4.3 Responsibilities

3.4.3.1 I/S Lighthouse User Group

The I/S Lighthouse User Group is responsible for:

- Content author assistance.
- Coordination of content and approvals.
- Content management for areas without content authors.

3.4.3.2 I/S Lighthouse Site Owners

The I/S Lighthouse Site owners are based on assignment of the ISPC chair and are responsible for:

- Ensuring that all information is accurate at content submission.
- Ensuring that ownership is established.
- Collecting management approval for publication.
- Adherence to ISSM standards and corporate style guide.
- Checking for content duplication and overlaps.
- Ensuring that links to the MPM and ISSM for the respective section are displayed on the home page for the I/S Processes group.
- Monitoring the progress of content prior to publication.
- Ensuring that content is reviewed and updated every 365 days at a minimum.

3.4.4 I/S Lighthouse Content

The general term document is used to describe any piece of content. It may refer to text within one of the I/S Lighthouse pages or an external entity that is displayable from the I/S Lighthouse.

All I/S Lighthouse content must meet the following standards:

- All content is published and accessible to I/S staff.
- Content must adhere to the Corporate Style Guide located on My e-Work.

3.4.5 Content Review

Content must be reviewed and recertified by the responsible, respective area annually. Expiration dates will be set to 365 days to ensure recertification. Reminders of expiration will be sent. The ISPC chairs will be responsible for ensuring that content is updated. Note that expired content is not automatically removed.

Chapter 4 The Information Systems Standards Manual

Under the direction of the Information Systems (I/S) Governor, the Information Systems Standards Manual (ISSM) contains the standards for all information systems-related activities within BlueCross BlueShield of South Carolina and its subsidiaries. For the consistent and rational development, deployment and maintenance of computer systems, the ISSM provides a comprehensive structure for processes and procedures.

4.1 ISSM Maintenance

4.1.1 ISSM Numbering and Reference Formatting

The ISSM uses dynamic numbering for chapters, sections, and all subsequent subsections. This means that if a new chapter or section is inserted between others, the numbering will automatically update in the published version. The ISSM is updated monthly; therefore, to refer to text in the ISSM, the format below (Table 4-1) must be used without numbering to minimize the need to update the reference.

ISSM Text Reference Format

Reference Location	Reference Target	Reference Detail to Use	Reference Detail Example
Unnumbered Subsection	Same Unnumbered Subsection, Numbered Section, Numbered Chapter and Volume	Low	For details on these deliverables, see [above/below] in this subsection.
Unnumbered Subsection	Different Unnumbered Subsection in the Same Numbered Section, Same Numbered Chapter and Volume	Medium	For details on these deliverables, refer to the subsection *Funding Level Estimate* [above/below].
Unnumbered Subsection	Different Numbered Section or Different Unnumbered Subsection in a Different Numbered Section in the Same Numbered Chapter and Volume	Medium	For details on these deliverables, refer to the [section/subsection] [*name*] [above/below].
Unnumbered Subsection	All Other Variations	High (Breadcrumb Trail)	For details on these deliverables, refer to *[Volume] > [Chapter] > [section] > [section/subsection]*.
Numbered Section	Same Numbered Section, Numbered Chapter and Volume	Low	For details on these deliverables, see [above/below] in this section.
Numbered Section	Different Numbered Section or Specific Unnumbered Subsection in the Same Numbered Chapter and Volume	Medium	For details on these deliverables, refer to the [section/subsection] [*name*] [above/below].
Numbered Section	All Other Variations	High (Breadcrumb Trail)	For details on these deliverables, refer to *[Volume] > [Chapter] > [section] > [section/subsection]*.

ISSM Text Reference Format

Reference Location	Reference Target	Reference Detail to Use	Reference Detail Example
Numbered Chapter	Same Numbered Chapter and Volume	Low	For details on these deliverables, see [above/below] in this chapter's introductory text.
Numbered Chapter	Specific Numbered Section or Specific Unnumbered Subsection in the Same Numbered Chapter and Volume	Medium	For details on these deliverables, refer to the [section/subsection] [*name*] [above/below].
Numbered Chapter	All Other Variations	High (Breadcrumb Trail)	For details on these deliverables, refer to *[Volume] > [Chapter] > [section] > [section/subsection].*
Volume (There would be no references at the Volume level.)	NA	NA	NA

Table 4-1 ISSM Text Reference Format

4.1.2 ISSM Annual Review

All content in the ISSM is required to undergo an annual review to determine if it is still applicable. This review must be completed within 365 days of the previous content review. The completion of each review will be recorded in the I/S Standards Committee (ISSC) meeting minutes. Any content that requires modification will be recorded and evaluated further.

The following table (Table 4-2) identifies who is responsible for reviewing ISSM content (e.g., a subcommittee of the I/S Policy Committee [ISPC]) and whether the content is in a **Vote** or **Non-Vote** section. These content distinctions are defined as follows:

- **Non-Vote** — Standards that **are related** to I/S Governance or Methodology and that **do not require a vote** from the ISSC to be published in the ISSM. Examples include standards on Adaptive Change, Enabling Processes, System Development Methodology, and those that support compliance to contractual regulations.
- **Vote** — Standards that **are not related** to I/S Governance or Methodology and that **do require a vote** from the ISSC to be published in the ISSM. The standards in this content are to be adhered to when working on I/S activities and include standards on coding, software configuration, tools and Incident Management.

ISSM Content Review

Volume	*Chapter > Section > Subsection*	Responsible ISSC Work Group or *Information Systems Department*	Responsible ISPC Subcommittee or *Information Systems Department*	Vote or Non-Vote Section
Adaptive Change	*I/S Standards > I/S Lighthouse*	I/S Lighthouse User Group	Enabling Processes Subcommittee	**Non-Vote**
Adaptive Change	*Audit Management*	*I/S Governance — Audit Management Office*	*I/S Governance*	**Non-Vote**
Adaptive Change	Rest of the Volume	*I/S Governance — Process Audit*	*I/S Governance*	**Non-Vote**
LOB Management	*Resource Acquisition*	Inventory Subcommittee	LOB Management Subcommittee & Service Management Subcommittee	**Non-Vote**
LOB Management	Rest of the Volume		LOB Management Subcommittee	**Non-Vote**
Enabling Processes	*Managing People Program > IT Roles and Other IT Roles*	*I/S Governance — Process Design*	Enabling Processes Subcommittee	**Non-Vote**
Client Management	All		Client Management Subcommittee	**Vote**
Systems Architecture	*Workstation Hardware/ Software*	Workstation Infrastructure Subcommittee	Systems Architecture Subcommittee	**Non-Vote**
Systems Architecture	*Concepts & Techniques*	*Enterprise Architect Office*	Systems Architecture Subcommittee	**Vote**
Systems Architecture	Rest of the Volume	*Enterprise Architect Office*	Systems Architecture Subcommittee	**Non-Vote**
Application Systems	*Application Systems*	*I/S Governance —*	*I/S Governance*	**Non-Vote**

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

ISSM Content Review

Volume	*Chapter > Section > Subsection*	Responsible ISSC Work Group or *Information Systems Department*	Responsible ISPC Subcommittee or *Information Systems Department*	Vote or Non-Vote Section
Management	*Management Framework*	*Process Design*		
Application Systems Management	Rest of the Volume		Project Management Subcommittee	Vote
Service Management	*Service Management Overview*		Service Management Subcommittee	Vote
Service Management	*Service Support > Incident Management* *Service Support > Problem Management*	Incident/Problem Management Subcommittee	Service Management Subcommittee	Vote
Service Management	*Service Support > Configuration Management > SharePoint Online*	*Corporate Applications*	Service Management Subcommittee	Vote
Service Management	*Service Support > Inventory Management*	Inventory Subcommittee	Service Management Subcommittee	Vote
Service Management	*Service Support* Remaining Sections		Service Management Subcommittee	Vote
Service Management	*Service Delivery*	Service Continuity Management Subcommittee	Service Management Subcommittee	Vote
ICT Infrastructure Management	All	Infrastructure Technical Standards Subcommittee	ICT Infrastructure Management Subcommittee	Vote

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

ISSM Content Review

Volume	*Chapter > Section > Subsection*	Responsible ISSC Work Group or *Information Systems Department*	Responsible ISPC Subcommittee or *Information Systems Department*	Vote or Non-Vote Section
Security Management	All		Security Management Subcommittee	Non-Vote
Technical Standards — Infrastructure	*Overall Technical Infrastructure Standards* *Appliances*	Application Technical Standards Subcommittee	Application Systems Management Subcommittee	Vote
Technical Standards — Infrastructure	Rest of the Volume	Infrastructure Technical Standards Subcommittee	ICT Infrastructure Management Subcommittee	Vote
Technical Standards — Applications	*Application Coding* *Application Systems Support* *Other Considerations* *Standards for Web-based Applications*	Application Technical Standards Subcommittee	Application Systems Management Subcommittee	Vote
Technical Standards — Applications	*Application Validation*		Application Systems Management Subcommittee	Vote
Technical Standards — Applications	*Application Development Support Tools*	IT Business Systems (ITBS) User Group	Application Systems Management Subcommittee	Vote
Technical Standards — Applications	*Business Systems Considerations* *File Management*	Infrastructure Technical Standards Subcommittee	ICT Infrastructure Management Subcommittee	Vote

ISSM Content Review

Volume	*Chapter > Section > Subsection*	Responsible ISSC Work Group or *Information Systems Department*	Responsible ISPC Subcommittee or *Information Systems Department*	Vote or Non-Vote Section
	Standards and Guidelines *File Design*			
Technical Standards — Applications	*Print Operations*	*I/S Print Operations*	Application Systems Management Subcommittee	**Vote**
Procedures & Tools	*Testing Tools*	Testing User Group	Application Systems Management Subcommittee	**Vote**
Procedures & Tools	Rest of the Volume	ITBS User Group	Application Systems Management Subcommittee	**Vote**

Table 4-2 ISSM Content Review

4.1.3 Recommendations from the Work Groups to the ISSC

Decisions reached by the ISSC work groups must be documented with justification and impact, and then presented to the ISSC by the ISSC work group chair (or a designee). Any modifications to existing standards or creation of new standards must be written and follow the process discussed in the section *Proposed Changes to the ISSM* below.

4.1.4 Proposed Changes to the ISSM

Listed below is the process for submitting changes to the ISSM:

1. Additions, modification or deletions to the ISSM can be presented by any staff member to the applicable ISSC subcommittee. The subcommittee will review the updates and determined if the ISSM should be updated. Once a draft is approved to go to the ISSC, the subcommittee chair will submit the changes to the ISSC Administrator at IS-QA-PROCESS-MGMT.
2. The submitted draft must follow these standards:

    a. Content related to the changes must be obtained from the latest version of the ISSM volume being changed. For this, contact the ISSC Administrator at IS-QA-PROCESS-MGMT. If the volume affected has been updated during the time that the draft is being developed, changes must be remade to the latest version of the volume.

b. Changes must be done in a Microsoft Word document using the Track Changes feature. Contact the ISSC Administrator for specific instructions on how to set up Word for items being submitted to the ISSC. If the changes are being reviewed and edited prior to submission to the ISSC, do not submit a copy with some of the tracked changes already accepted. All changes must be visible at the time of submission in order to ensure that they are properly incorporated into the ISSM upon approval.
c. The draft should include a summary of the updates along with a reason for the change.

3. The ISSC Administrator distributes the agenda for the monthly ISSC meeting to all the members of the ISSC. The agenda includes any proposed changes to the ISSM. The item is presented to the ISSC during **1st Read** by the subcommittee chair or staff member (or a designee if deemed necessary) mentioned in step one (1) above. The ISSC members will discuss each proposed recommendation or change with the I/S area they represent and solicit input.
4. At the next scheduled ISSC meeting, the original staff member (or a designee) recaps the draft to the ISSC and mentions any feedback received **(2nd Read)**. If the individual submitting the proposed change fails to show for two consecutive ISSC meetings, the proposed change/recommendation will be removed from the agenda.
5. The ISSC is responsible for approving the proposed changes, which are classified as either votable or non-votable. If a vote is required for the changes, the ISSC Administrator polls the voting representatives. As long as there is no opposition to the proposed changes, non-votable changes are approved without a vote. Approved standards are published to the ISSM by the end of the month.
6. Depending on the complexity of the change, the ISSC may defer voting until the issue can be properly researched. The ISSC Chair will appoint a task force to investigate the issue and develop recommendations for the next ISSC meeting.

4.1.5 Cosmetic Changes

Additions, modifications or deletions involving grammar, punctuation, spelling, capitalization, hyperlinks, references and formatting (e.g., paragraph alignment, spacing, and general appearance) are classified as *cosmetic changes*, and they will be reviewed by the ISSC Chair for initial approval. Once approved, the cosmetic changes will be presented to the ISSC for a 1st Read. In order to expedite these types of changes, the ISSC Chair will reserve the right to waive the need for a 2nd Read or, if applicable, a 2nd Read and a vote by the ISSC and proceed with giving final approval on the changes. The ISSC Administrator will notify the ISSC if the cosmetic changes will only have one Read.

During an approved update of the ISSM, the ISSC Administrator or an I/S Governor designee has the editorial license to make needed cosmetic changes that have been identified in the update, in the surrounding content, or both. Those cosmetic changes that are not related to punctuation, capitalization, spelling or formatting will be disclosed to the ISSC either prior to publication or at the next monthly meeting.

Chapter 5 Process Audit

Under the direction of the CIO, the Process Audit department examines, evaluates and analyzes the internal standards, processes and I/S Management procedures of the BlueCross BlueShield of South Carolina organization. The purpose of this analysis is to determine if the standards, processes and procedures are working effectively to improve the overall performance of the organization while fulfilling all related contractual and government audit requirements.

5.1 Waivers

There may be instances in which standards in this manual do not accommodate a specific situation and judgment is required on how to handle the situation. In order to accommodate these situations, the I/S Governor or designee is empowered to approve deviations from a published Information Systems standard.

To request a waiver, the requestor must document the waiver request in the form of an email. The email should contain the standard to be waived along with the rationale justifying the need for the waiver. The requestor should obtain their management's agreement and then forward the waiver request email to Process Audit at IS-QA-PROCESS-MGMT to obtain I/S Governance approval.

The requestor will be notified of the decision via email.

5.2 Standards Review

The Process Audit department performs a number of functions related to the ISSM standards, government controls and other business standards. The department:

- Maintains the ISSM and conducts an annual review of the content.
- Randomly conducts reviews during and after the development process in order to:
    - Suggest methods for improving quality.
    - Help identify critical failure points within the development processes.
    - Provide and obtain feedback on how the processes can be modified to increase the probability of quality results.
- Conducts random audits of any of the processes, methodologies or standards within the ISSM.
- Evaluates and approves waivers to standards.
- Conducts CIO- and Executive Management-directed audits and process reviews.
- Monitors local admin rights.
- Monitors the use of unauthorized software and validates the approved software listing.
- Monitors software configuration management-approver groups that have been set up for Host and Non-Host.

Chapter 6 Global Standards

6.1 Reviews

6.1.1 Periodic Reviews

One of the vital requirements of BlueCross BlueShield of South Carolina (BlueCross) Application Systems Management (ASM) Framework is to ensure that focused, effective communication occurs between the participating parties at significant points throughout the life cycle of a work effort. Reviews should be conducted during the phases within the ASM Framework with all stakeholders identified during the Discovery and Delivery Strategy. This will ensure that there is effective communication throughout the life cycle of the work effort and the necessary approvals are received.

During a review, information should be shared regarding the direction and progress of an activity or documentation to ensure that the involved parties understand and agree on what's being delivered, why, when, where and how. The review ensures that the work products meet the specified requirements and are consistent with documentation developed earlier in the methodology.

Reviews may take many forms, ranging from formal meetings to conference calls, to exchanging emails. It is essential that all parties involved in the reviews receive the proper related deliverables, participate in the reviews, and concur with all conclusions and findings. All areas participating in a review must document their concurrence or non-concurrence with the activity or documentation presented. This is also known as receiving a *sign-off*.

The Project Manager organizes the reviews involving most or all of the Work Request Team members. For those reviews that are more focused, such as, but not limited to, code compliance reviews and solution package or wireframe reviews, the review organizer is typically the author or creator of the artifact or activity being reviewed.

For the major phase deliverables, such as the Discovery and Delivery Strategy, Design/Development/Validation, Go-Live or Implementation Plan Reviews, the organizer should not assume an area is not involved, but receive confirmation from each area regarding its level of involvement. Once the list of participants for a given area is determined, invited participants need to confirm that they can fully represent their area’s interests. If there is any question, I/S Management should be contacted to supply additional representatives or a substitute who can represent the given area.

All review documents and the concurrence are forwarded to the Project Manager who then stores them in the ***SharePoint Online (SPO)*** site for the Work Request.

6.1.2 Architectural Reviews

There are several artifacts that require Enterprise Architect approval. These include, but are not limited to, Concept Diagrams, Technical Architecture Documents, Service Creation Requirements, Bridge Diagrams, and Final Customer Summary Documents. The Enterprise Architect may require that any other artifact has this approval.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

These I/S-only Architectural Reviews follow a slightly different sequence of events than the usual review. The sequence of events is described below. Any changes made after the Enterprise Architect approval must follow the same Architectural Review again.

- The Role responsible for delivery of the artifact conducts the usual review with peers, Work Request Team members as listed in the artifact descriptions, and the Work Request technical leadership, the Solution System Designer or the Infrastructure Solution Designer, as appropriate.
- Once approved, the technical leadership presents the artifact to the Architect.
- Once approved the Architect presents the artifact to the Enterprise Architect for final approval.

6.2 Methodology Documentation — Overview

The documentation for the methodology is called "development" or "life cycle" documentation. Life cycle documentation is created and maintained during the life of a given Work Request for product development. It is associated with methodology deliverables, reviews, or relevant information that occurs during the development processes. Work Request life cycle documentation resides in the ***SPO*** system.

6.2.1 Documentation Confidentiality Disclaimer

Each page of life cycle and systems documentation should contain a confidentiality disclaimer to protect BlueCross BlueShield of South Carolina information. Unless your area has a confidentiality statement approved by the Law Department, the following statement should appear throughout your documents:

This material is the confidential, proprietary and trade secret product of BlueCross BlueShield of South Carolina and any affiliates or subsidiaries it directly or indirectly controls (BlueCross). Any unauthorized use, reproduction or transfer of these materials is strictly prohibited.

Copyright YYYY BlueCross BlueShield of South Carolina. All rights reserved.

(Where YYYY equals current year)

Chapter 7 Standards for Non-I/S Areas

The purpose of this section of the ISSM is to provide a policy concerning the development and maintenance of I/S development standards for information systems that are not directly supported and managed by the Information Systems Division of BlueCross BlueShield of South Carolina (an example is Palmetto GBA Medicare Systems). I/S areas not in the Information Systems Division may follow the ISSM standards, rather than developing and maintaining their own standards.

Any I/S area not under the Information Systems Division that interacts with the BlueCross BlueShield of South Carolina Corporate Data Center (CDC) or the Companion Data Services (CDS) Data Center or with the staff of the I/S Division must follow the ISSM standards for those interactions.

7.1 Software Development/Maintenance Responsibilities

It is the responsibility of any other I/S area installing, maintaining, or developing software systems, which are not part of the Information Systems Division supported set of systems, to develop and maintain standards that cover the following topics. In addition to the topics outlined below, that I/S area will identify any other topic specific to their environment that would require the development of appropriate standards.

Application Systems Design and Programming

- System design considerations
- Program design considerations
- Program coding considerations
- System testing/production system modification procedures

System Operation

- System hardware profile
- Job Control Language (JCL) standards (Hardware equivalent)
- System naming conventions
- Source management standards and procedures
- File management standards and procedures
- System utilities description and use

Computer System Operations Manual

- Working hours/hours of operation
- Preventative maintenance
- IPL/shutdown procedures
- Powering on/down procedures
- Execution control
- Restart failures
- A/C — power failure
- Printers
- Disks
- Tapes
- Reader/punch
- Computer Center disaster procedures
- Computer Center security procedures
- Fire protection system

System Disaster Recovery Manual

- Recovery team structure
- Data backup and off-site storage procedures
- Plan initiation/escalation procedures
- Emergency procedures
- Disaster recovery plans/procedures
- Critical applications
- Plan test procedures

- Appendix

System Security Manual

- Secured area policy
- Physical facilities
- Computer room access
- Computer processing
- Online system security procedures
- Available transactions
- Security system

7.1.1 Administration

The information described above must be developed and maintained in a manual format. Further, these manuals become part of Corporate I/S Policy and are governed by the ISSC and the CIO. Once the ISSC and the CIO approve the original manuals, any additions/changes to the manuals must follow the procedures outlined in *Adaptive Change > The I/S Standards Manual > ISSM Maintenance > Submitting Proposed Changes to the ISSM.*

7.2 End-User Computing

The purpose of this section is to document the standards that govern the development, use, and procurement of software by our end users. Information Systems (I/S) generally supports all software that is necessary to support core business operational needs. However, there are occasions when the end users may have unique business needs and may choose to develop their own software or procure a commodity software. In these cases, the end-user developed or procured software must only address reporting, information gathering or analytical needs and not core operational issues, such as claims processing or membership (enrollment or billing).

All infrastructure hardware and infrastructure software associated with end-user supported software must be provided and supported by I/S unless otherwise authorized by the CIO.

7.2.1 End-User Supported Software

The end-user supported software owner will be required to provide all of the following support activities that include, but are not limited to:

- User training
- Release/version upgrade evaluations
- Software configuration management of object/source code
- Business continuity support
- Security compliance
- Audit inquiries
- Help desk support
- Software license agreement
- Software license compliance
- Compatibility testing with infrastructure hardware and software upgrades

The end-user supported software must be technically sound and meet all security requirements. In addition, the software must follow these guidelines:

- If the end-user supported software is to be either utilized by multiple users via the Corporate Network (I/S LAN/WAN), or to house related data, I/S approval is required to evaluate the software or data technical compatibility and any performance impacts it may have on the network. Approval should be coordinated by a Client Advocate using the Vendor Alert Process. Refer to *Systems Architecture* > *General Architectural Standards* > *Vendor Software Usage* > *Vendor Alert Process* for details.
- If an end-user supported software fails to follow the above guidelines and causes performance, stability or support issues, I/S may disable the application without warning.

7.2.2 End-User Supported Software Procurement

All end-user supported software must be purchased through BlueCross BlueShield of South Carolina and approved by I/S. I/S must also approve any software that is obtained outside of a formal purchasing process (e.g., freeware obtained through the Internet) prior to it being loaded and utilized. Please refer to *Systems Architecture* > *General Architectural Standards* > *Vendor Software Usage* for additional information.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

7.2.2.1 Installation of End-User Supported Software

A support technician from the authorized I/S Workstation Support organization must install all end-user supported software loaded on a BlueCross BlueShield of South Carolina workstation to ensure standard software installations and configurations are adhered to.

Chapter 8 Audit Management

8.1 Overview of the Audit Management Office

The I/S organization is subject to being audited by entities both internal and external to the company. The Audit Management Office (AMO) ensures that audits can be conducted concurrently with the day-to-day activities within I/S. The AMO executes processes related to planning, monitoring and controlling, and managing the Audit Request Methodology to ensure that Audit Requests are completed on time, within budget, adhere to high quality standards, and to ensure that all audit findings or observations are either successfully rebutted or remediated. An analogy can be drawn between the Audit Management Leader for audits with the Project Manager for the Application Systems Management (ASM) Framework Work Requests in that the Audit Management Leader provides the leadership role within I/S for the Audit Request Methodology.

The primary responsibilities of the AMO are:

- **Managing Audit Requests —** Ensure that the Audit Request Methodology is followed on all I/S Audits.
- **Remediation Tracking —** Track all corrective actions necessary to remediate audit findings.

Once audits are completed, the AMO continues to perform follow-up activities to ensure that all items in the consolidated list of remediation activities (Corrective Action Plan) are addressed in the timelines established.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

8.2 Audit Request Management

8.2.1 Ongoing Life Cycle Requirements

The Audit Management Leader is responsible for the following life cycle requirements that continue throughout the Audit Request process:

- Audit status is updated in MPS.
- Issues, risks and tasks are monitored.

8.2.2 Steering Support Process

The Steering Support process is the input to the Audit Request Management processes. The Steering Support process for audits is identical to what is described for other Work Requests found in *Client Management > Steering Support*. When Client Management receives notification that an audit of I/S will be performed, they open a Work Request under the appropriate steering committee.

8.2.3 Audit Request Management Processes

8.2.3.1 Audit Definition Process

The Audit Definition Process is similar to the Work Definition Process described in *Application Systems Management > Project Management > Work Request Management > Work Definition*. Client Management coordinates the activities for this process.

Client Management works with the Auditor to initially define the audit. There are times where the scope of the audit can be well defined upfront, but there are other times when the Auditor may need to gain an understanding of the internal processes before the scope of the audit can be finalized. If the criteria are well defined, an authorization level of "Combined Discovery/Audit Planning Phases" can be selected on ***MPS***. If the Auditor needs to become familiar with BlueCross processes first, the Discovery phase will be conducted before the Audit Planning Phase, and the Audit Request will be designated as "Separate Discovery/Audit Planning Phases" on ***MPS***.

The Client Advocate completes a Work Definition Document (WDD) that outlines as much information that is available. If there is a requested start date and a known length of time for the audit, this should be included in the WDD, as it will assist the areas being audited to determine impacts and provide high level estimates.

8.2.3.2 Estimate

The Estimate processes documented in *Application Systems Management > Project Management > Work Request Management > Estimating* also apply to Audit Requests, with the following differences:

- Risk alerts do not apply.
- Funding Level Estimates are not an option.

When estimates are being provided, historical actual hours should be considered if a similar audit was performed in the past, and the same areas are impacted.

8.2.3.3 Scheduling

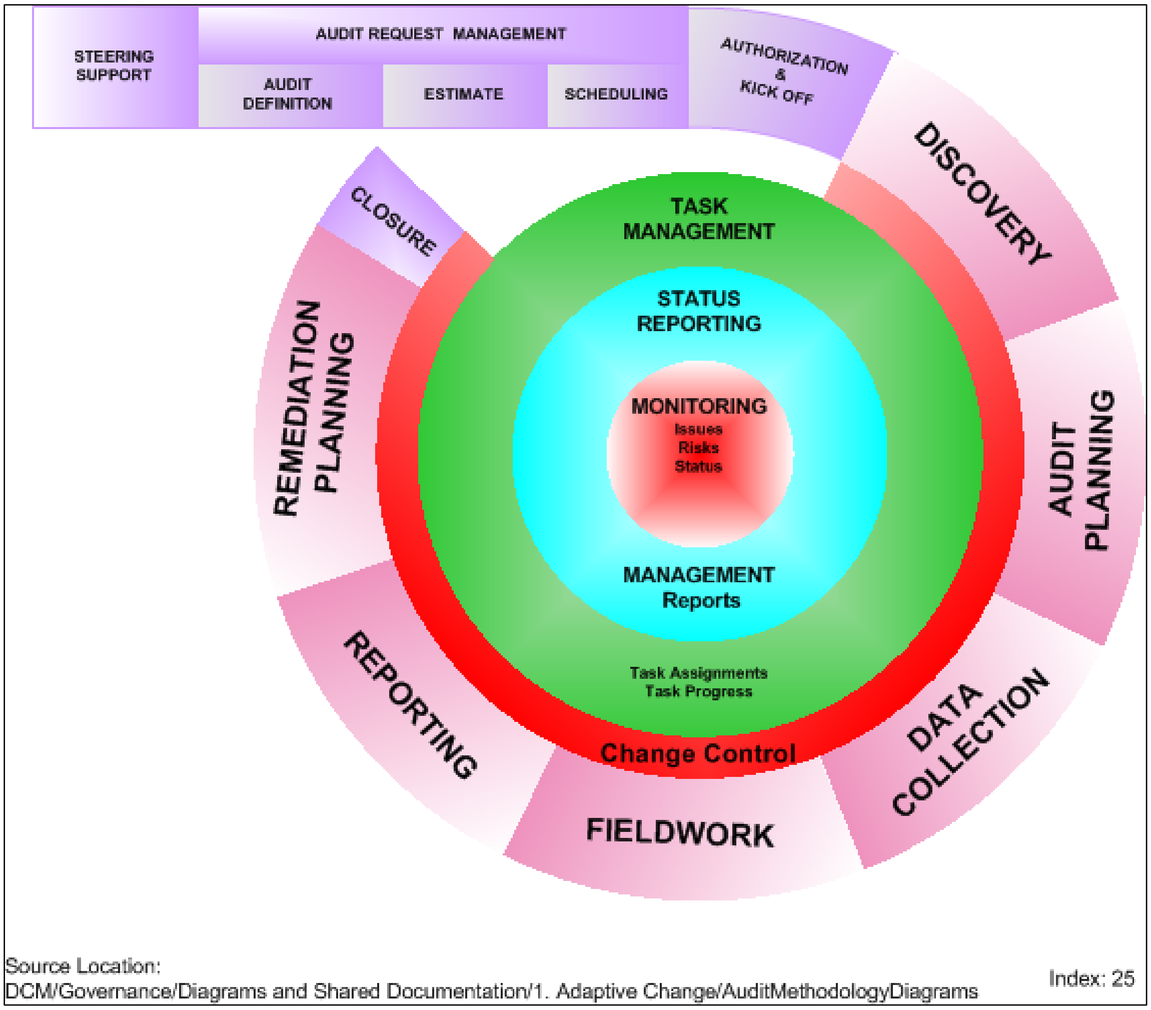
The scheduling process documented in *Application Systems Management* > *Project Management* > *Work Request* > *Scheduling* also applies to Audit Requests. The purpose of the scheduling process is to set a start date for the effort when all impacted areas can have resources available. However, for external audits, the auditing agency may specify when they will be on-site to conduct the audit, and the date may not be negotiable. In these cases, the systems areas impacted by the audit may need to reschedule their workloads to accommodate the mandated start date. The system managers will need to coordinate with the Client Management organizations to determine how to reschedule the existing workload and initiate change control on those efforts.

8.3 Audit Request Methodology

8.3.1 Purpose of Audit Request Methodology

The intent of the Audit Request Methodology is to standardize the process for I/S involvement in audits so that audits are recognized as one of the core units of work and can be properly planned and resources adequately scheduled. The intent of this methodology is not to define how audits are to be conducted. The Auditor determines the process that will be used for the audit (the "audit program" or "testing plan"). Instead, the Audit Request Methodology defines the expectations and deliverables of I/S during the course of an audit and helps communicate the status of the audit based on achieving defined milestones.

8.3.1.1 Overview of Audit Request Life Cycle



Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams

Index: 25

Figure 8-1 Audit Request Life Cycle

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

Audit Request Management — Processes related to Audit Definition, Estimate, and Scheduling for Audit Requests

- **Audit Definition** — Processes related to defining the scope of the Audit Request.
- **Estimate** — Processes related to the estimation of effort to complete a given Audit Request.
- **Scheduling** — Processes related to planning and scheduling a given Audit Request for completion.

Audit Request Methodology — Processes supporting a structured execution (life cycle) defining the expectations and deliverables of I/S during the course of an audit (see **Figure 8-1** above).

- **Discovery** — Processes related to gaining an understanding of the application or process that is to be audited so that the scope of the audit can be determined.
- **Audit Planning** — Processes related to refining estimates, schedules and resource plans by I/S so that the appropriate level of support can be provided for the remainder of the audit.
- **Data Collection** — Processes related to the gathering of any documentation or reports required to conduct the audit activities.
- **Fieldwork** — Processes related to the auditing of the defined processes and/or artifacts against the established criteria, and the testing of control objectives.
- **Reporting** — Processes related to the publishing of audit findings and the creation of responses and Corrective Action Plans to the findings.
- **Remediation Planning** — Processes related to ensuring that each corrective action has clear ownership and that the appropriate work effort is initiated for each item in the Corrective Action Plan.
- **Closure** — Processes related to finalizing the Audit Request on ***MPS***.

Task Management, Status Reporting and Monitoring — Processes performed throughout the life cycle by the Audit Management Leader to manage tasks, monitor issues and risks, and produce status reports to keep the I/S Points of Contact (POCs) up-to-date on the audit's progress.

Change Control — Processes to reset expectations of all involved parties when there is a significant change regarding the scope of the audit, the estimated hours, the milestone deliverable dates or the duration of the audit. There may be times during the audit when additional, seemingly unrelated, questions and issues arise that need to be addressed or clarified. If significant time or resources are required, a change control should be executed to allow for additional time and I/S resource planning. The Audit Management Leader will coordinate change control with the audit participants and obtain agreement from Client Management before presenting to the Auditor.

8.3.1.2 Audit Request Methodology Summary Matrix

The chart below (Table 8-1) provides a summary of deliverables for each of the execution phases of the Audit Request Methodology.

Audit Request Methodology Summary Matrix

Audit Phase	Audit Deliverable
Discovery	• Audit Scope Statement from Auditor • Audit Program or Testing Plan from Auditor • List of items from Auditor needed to conduct audit
Audit Planning	• Updated I/S Estimate and Audit Schedule
Data Collection	• I/S-Provided Requested Artifacts
Fieldwork	• Audit Findings or Observations from Auditor • Exit Meeting (external audits only)
Reporting	• Draft Report from Auditor • I/S Management Responses
Remediation Planning	• I/S Corrective Action Plan (CAP) • Work Initiation for Remediation Activities
Closure	• Final Report from Auditor • Closed Work Request Code

Table 8-1 Audit Request Methodology Summary Matrix

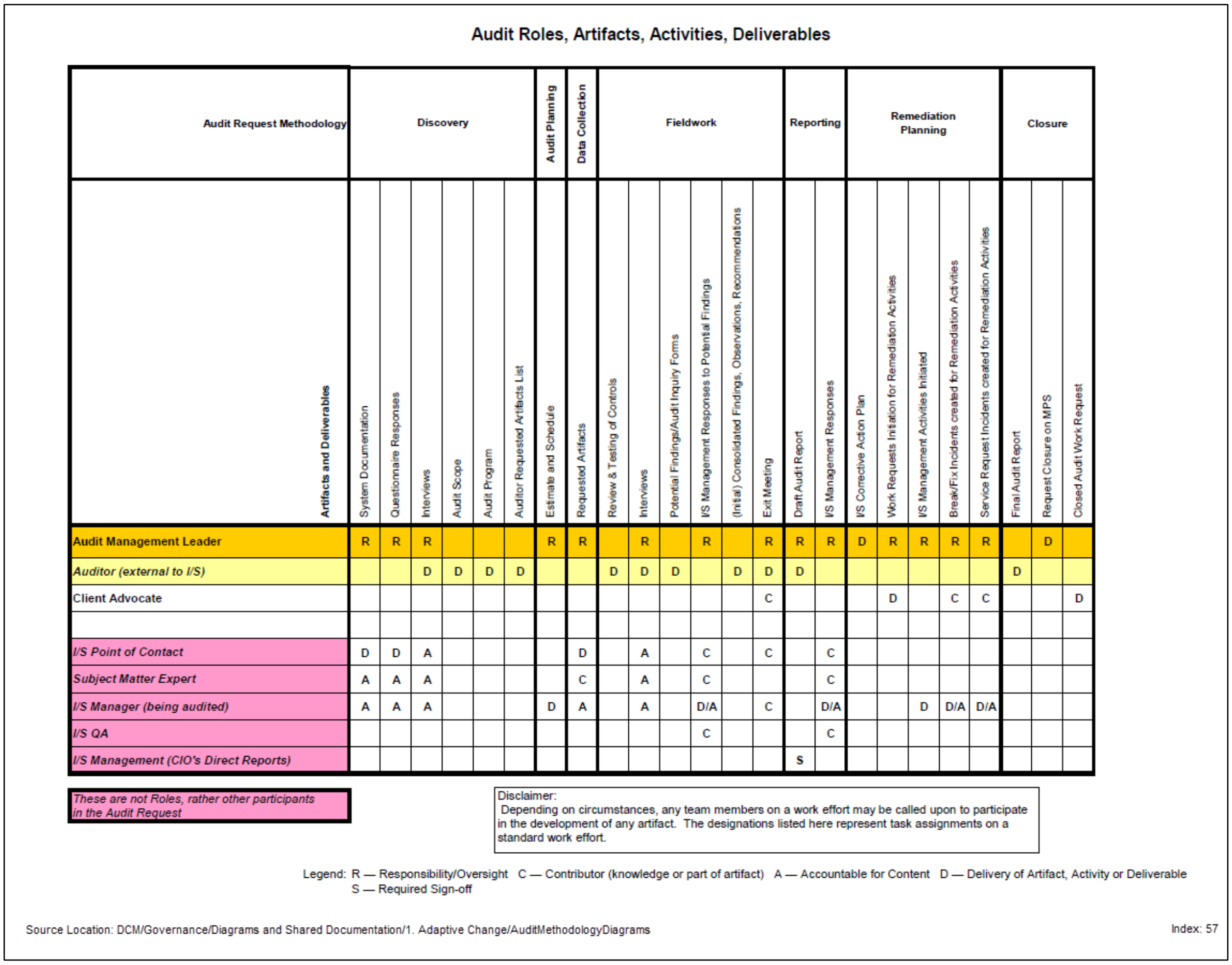
8.3.2 Audit Role

In keeping with the specialization of Information Systems, there is one Role defined for the Audit Request Methodology, and it is that of the Audit Management Leader. There are several other participants in the Audit Management Methodology. These participants are providing support to the Audit Request Methodology but do not have formal Roles, as their participation is limited and done in addition to their usual assignments.

Refer to *Enabling Processes* > *Managing People Program* > *IT Roles* > *Detail Role Descriptions* for a detailed description of the Audit Management Leader Role.

8.3.3 Audit Request Methodology Phases

In this section, the phases of the Audit Request Methodology are described. The Audit Accountability Matrix depicting the typical artifacts for an Audit Request is provided below (Figure 8-2, next page).



Audit Roles, Artifacts, Activities, Deliverables

Audit Request Methodology	Discovery						Audit Planning	Data Collection	Fieldwork						Reporting		Remediation Planning					Closure		
Artifacts and Deliverables	System Documentation	Questionnaire Responses	Interviews	Audit Scope	Audit Program	Auditor Requested Artifacts List	Estimate and Schedule	Requested Artifacts	Review & Testing of Controls	Interviews	Potential Findings/Audit Inquiry Forms	I/S Management Responses to Potential Findings	(Initial) Consolidated Findings, Observations, Recommendations	Exit Meeting	Draft Audit Report	I/S Management Responses	I/S Corrective Action Plan	Work Requests Initiation for Remediation Activities	I/S Management Activities Initiated	Break/Fix Incidents created for Remediation Activities	Service Request Incidents created for Remediation Activities	Final Audit Report	Request Closure on MPS	Closed Audit Work Request
Audit Management Leader	R	R	R				R	R		R		R		R	R	R	D	R	R	R	R		D	
Auditor (external to I/S)			D	D	D	D			D	D	D		D	D	D							D		
Client Advocate														C				D		C	C			D
I/S Point of Contact	D	D	A					D		A		C		C		C								
Subject Matter Expert	A	A	A					C		A		C				C								
I/S Manager (being audited)	A	A	A				D	A		A		D/A		C		D/A			D	D/A	D/A			
I/S QA												C				C								
I/S Management (CIO's Direct Reports)															S									

These are not Roles, rather other participants in the Audit Request

Disclaimer:
Depending on circumstances, any team members on a work effort may be called upon to participate in the development of any artifact. The designations listed here represent task assignments on a standard work effort.

Legend: R — Responsibility/Oversight C — Contributor (knowledge or part of artifact) A — Accountable for Content D — Delivery of Artifact, Activity or Deliverable S — Required Sign-off

Source Location: DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams

Index: 57

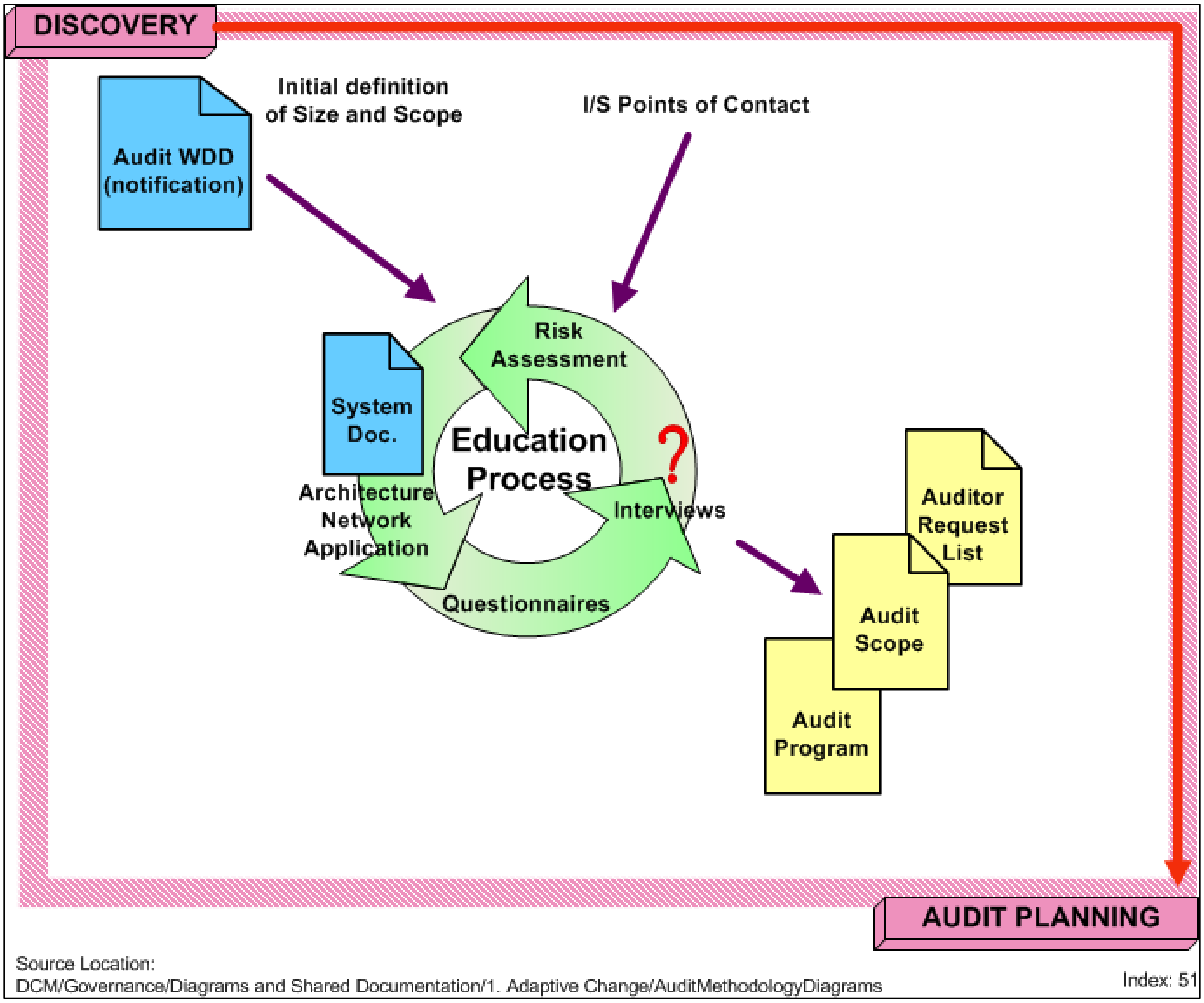
Figure 8-2 Audit Accountability Matrix

8.3.3.1 Audit Request Kick-Off Phase

This brief, administrative phase begins on the start work date that was determined in the scheduling process. The Audit Management Leader begins scheduling the necessary meetings or work sessions and notifies the I/S Points of Contacts (POCs) for each I/S area. The I/S POCs, Audit Management Leader and the Auditor set a milestone date for completing the next phase of the Audit Request.

8.3.3.2 Discovery Phase

The purpose of the Discovery Phase (see Figure 8-3) is to allow the Auditor to learn more about BlueCross internal processes, so that they can determine the scope of the audit that will be performed. During this optional phase, Auditors can gain more insight into I/S internal processes, review system documentation for the particular audited area, perform risk assessments, research and review regulations (Government, ISSM, etc.), and hold interviews with identified I/S POCs.



Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams

Index: 51

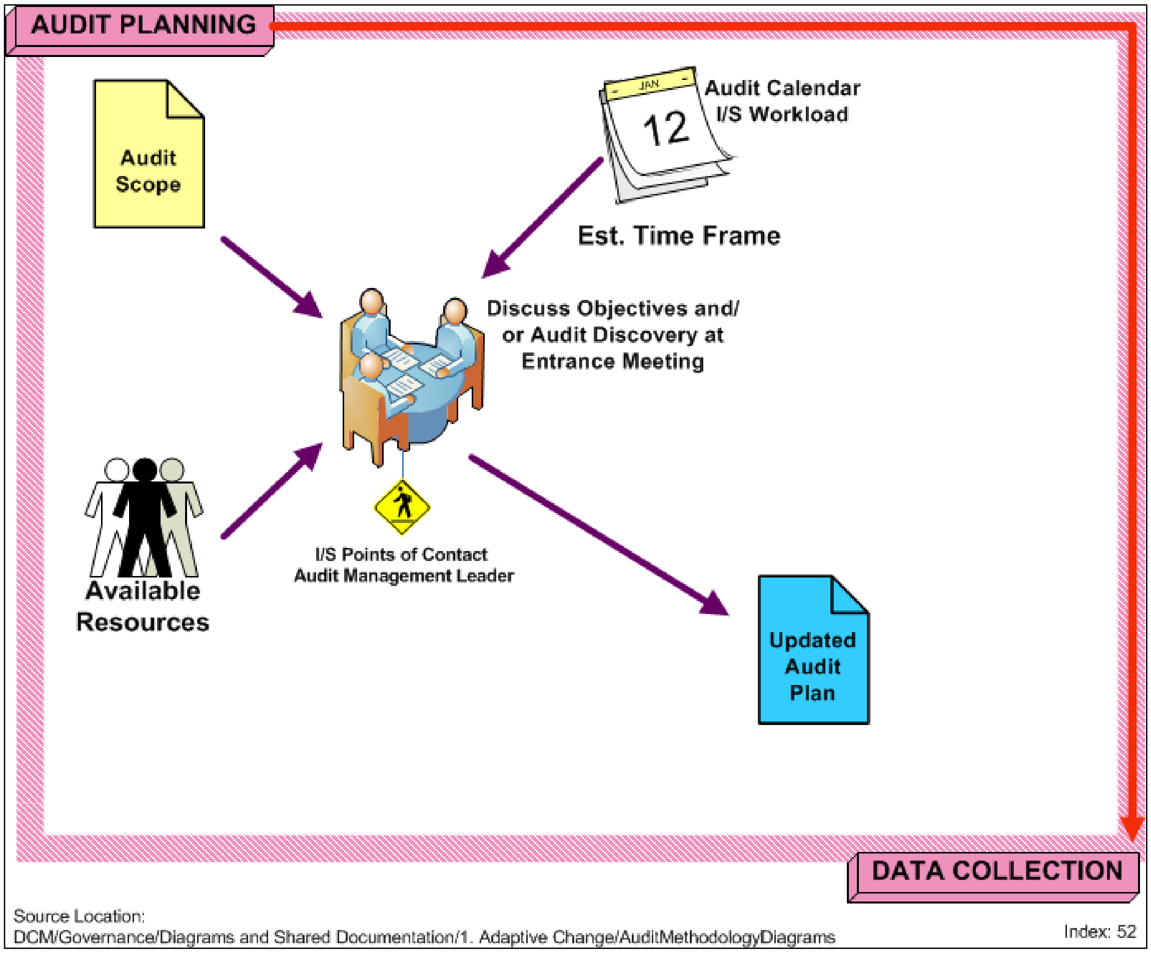
Figure 8-3 Discovery Phase

The Education Process is not required for all audits. For many external audits, the scope of the audit is well defined, and the Discovery Phase may be quite short. The information gathered in the education process helps to further refine the scope of the audit. Upon completion of the Discovery Phase, the actual audit may begin right away or may be scheduled for a future start date depending on resources or other constraints.

The deliverable for this phase is the Audit Scope Statement from the Auditor and possibly an Audit Program or Testing Plan that outlines how the Auditor will conduct the audit. The Auditor may also request a list of items that will be needed to conduct the audit (policies, procedures, manuals, etc.). The Audit Management Leader distributes this information to all impacted parties to allow them to determine the impact to their areas. The impacted area is then responsible for providing the listed items for which they have responsibility.

8.3.4 Audit Planning Phase

At the beginning of this phase (see Figure 8-4), the impacted I/S areas meet to review the updated Audit Scope Statement and ensure that everyone understands the expectations. The impacted I/S areas can then assess the level of effort required to support the audit and plan resources accordingly.



Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams
Index: 52

Figure 8-4 Audit Planning Phase

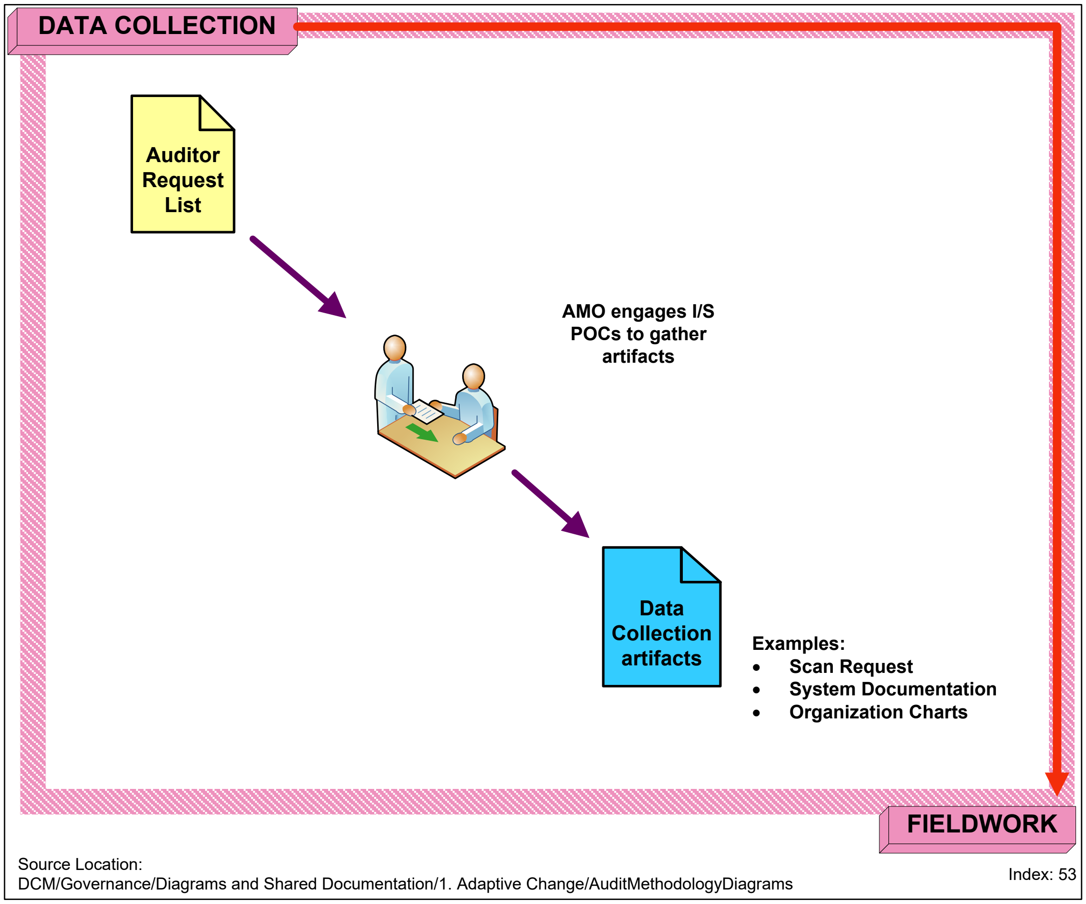
The deliverable from this phase is an updated estimate in hours and a schedule with milestone dates for completing the remaining phases of the Audit Request. The information from this Updated Audit Plan is then entered into ***MPS***.

8.3.5 Data Collection Phase

The Data Collection Phase (see Figure 8-5, next page) includes activities by I/S to gather any items that the Auditor has requested up to this point. For external audits, a list of required documents is provided by the Auditor. For internal audits, much of this information may be gathered during the Discovery Phase. During audits involving procedure reviews, the I/S points of contact (POCs) must identify the location within the Security, Risk and Compliance (SRC) system of applicable documents. If the necessary documentation is not already included in the SRC system, the I/S POC is responsible for ensuring that the documentation is uploaded.

The phase is considered to be complete once all of the artifacts on the original request list have been delivered.

NOTE After the Data Collection Phase is completed, the Auditor may determine that additional items need to be reviewed. The activity of collecting data can occur in any phase of the Audit Request Methodology.



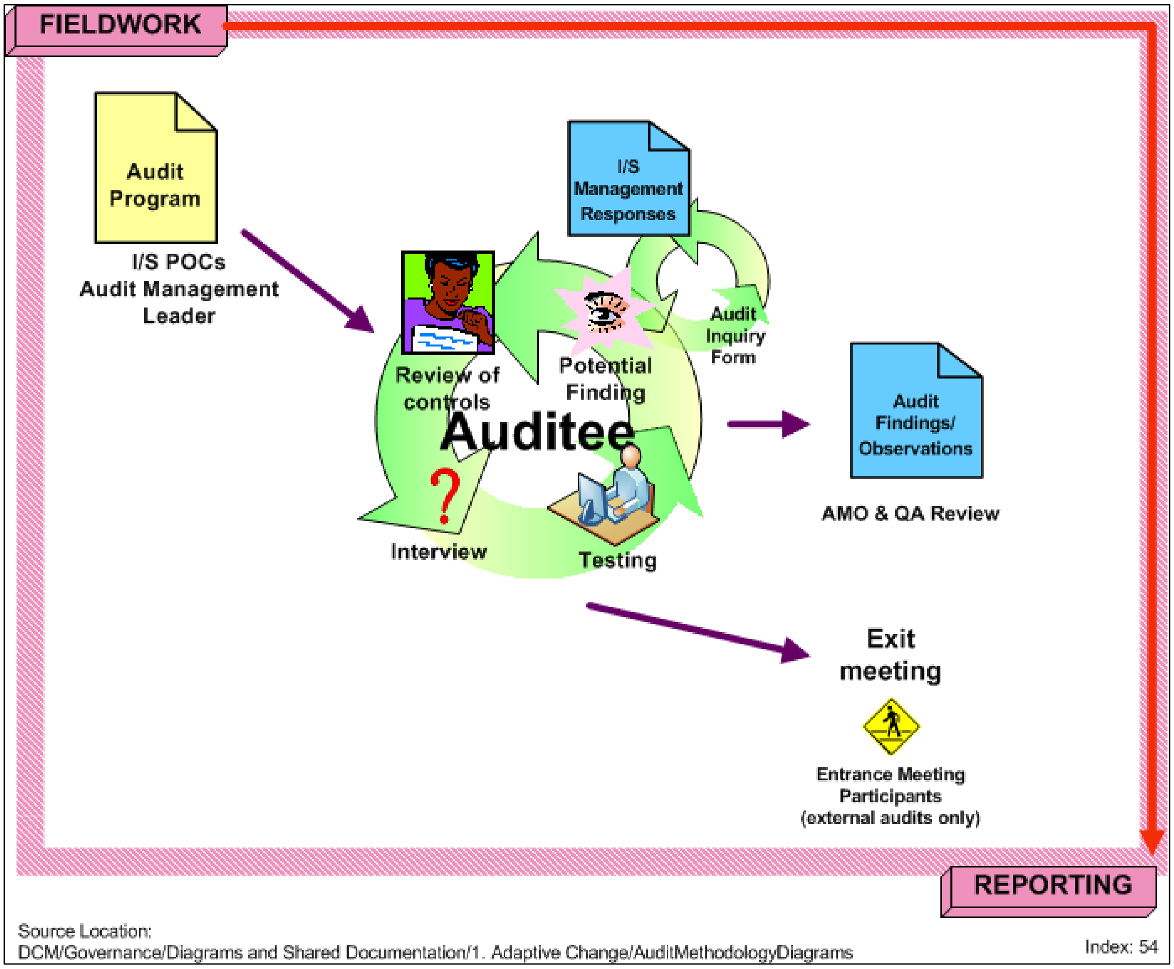
Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams

Index: 53

Figure 8-5 Data Collection Phase

8.3.6 Fieldwork Phase

This phase of the Audit Request Methodology (see Figure 8-6, next page) consists of the Auditor executing the audit Program or Testing Plan. This may include the Auditor reviewing artifacts and documentation, testing controls and interviewing the I/S POCs. During this phase, I/S is providing support to the Auditor by providing documentation and answering questions.



Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams

Figure 8-6 Fieldwork Phase

8.3.6.1 Potentially Reportable Issues

During the Fieldwork Phase, the Auditor may begin notifying the I/S POCs of "potentially reportable issues." These are possible findings or observations that the Auditor has that may be able to be clarified during the Fieldwork Phase. If so, then the issue will not appear in the audit report. For audits conducted by the BlueCross internal Corporate Audit Department, an Audit Inquiry Form is used by Corporate Audit to notify the I/S POCs of these issues. I/S POCs and the Audit Management Leader should strive to clarify the issue for the Auditor or provide additional documentation to resolve the issue during the Fieldwork Phase.

If I/S Management concurs with the finding or observation, they can begin developing the I/S Management response and Corrective Action Plan that will be required in the Reporting Phase. Any written responses should be coordinated through the Audit Management Leader. Responses provided during this phase will later appear in the draft audit report.

8.3.6.2 Exit Meeting

For external audits, an exit meeting is held prior to the departure of the external audit team from the BlueCross BlueShield of South Carolina site to recap the activities of the Fieldwork Phase of the audit. A recap of the fieldwork and current reportable issues will be reviewed with the I/S POCs.

The list of participants in the Exit Meeting should include:

- I/S Points of Contact.
- Audit Management Leader.

8.3.7 Reporting Phase

During this phase (see Figure 8-7, next page), the Auditor will issue a Draft Report that provides a summary of the work completed during the audit. The report will most likely include the following:

- An executive overview of the audit Program or Testing Plan
- The participants in the audit
- Any audit findings or observations
- Possible recommendations for improvement

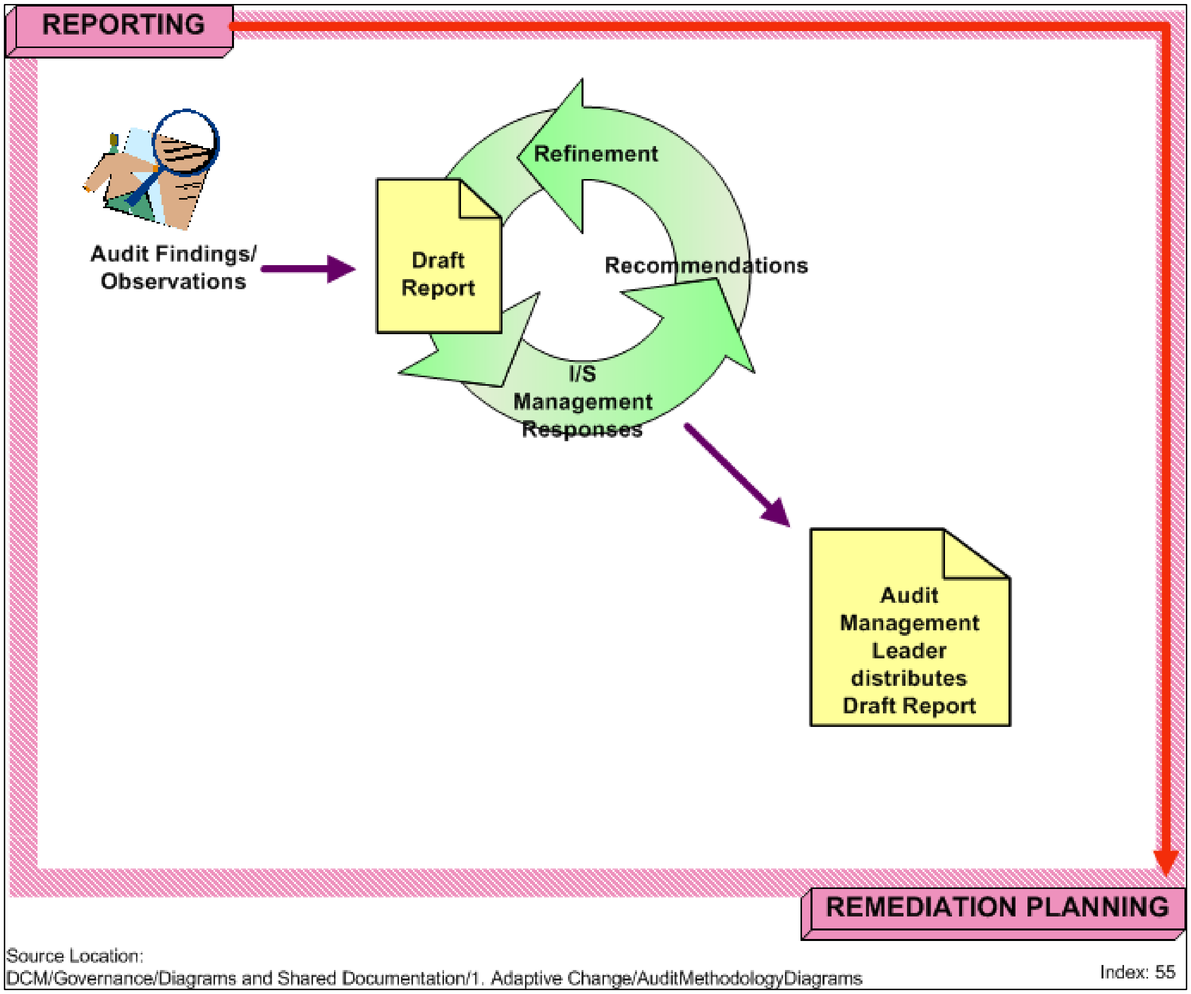

REPORTING
Audit Findings/ Observations
Draft Report
Refinement
Recommendations
I/S Management Responses
Audit Management Leader distributes Draft Report
REMEDIATION PLANNING
Source Location:
DCM/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams
Index: 55

Figure 8-7 Reporting Phase

The purpose of reporting the audit findings or observations is to provide clear communication of the audit findings to all parties involved. An audit finding or observation should describe the control, the standard which the control was measured against, and what is lacking with that control. Other information such as how the control was tested, participating personnel, and other supporting documentation may also be included.

The Audit Management Leader forwards the Draft Report to applicable I/S Management and solicits responses, if not already received during the Fieldwork Phase. There may be multiple iterations to refine the observation(s), recommendations and I/S Management responses between the Auditors and I/S.

Once the Draft Report is complete, signatures from the CIO's management team, the Direct Reports will be requested. The phase will be considered complete once the Audit Management Leader has distributed the last version of the Draft Report.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.

8.3.7.1 Management Response to Findings

Prior to responding to an audit finding or observation, it must be determined if the issue in question is a compliance issue (e.g., not following corporate policy, ISSM or departmental procedures) or if the issue is a risk-based control from an industry best practice, such as the National Institute of Standards and Technology (NIST) Special Publications or the Control Objectives for Information and Related Technologies (COBIT).

If it is not clear if the finding is a compliance issue or a risk-based control observation, the Audit Management Leader should ask the Auditor for clarification. The Process Audit department will review all compliance issues to validate that the corporate policy or ISSM standard was applied correctly. They will also help determine if the finding needs to be addressed at the area level where it originated or if the finding is a global issue that applies to all of I/S. This will help determine who should supply the I/S Management response.

If there are any risk-based control findings, the appropriate I/S Policy Committee subcommittee may need to be engaged to determine if an existing policy needs to be modified or if a new policy needs to be put into place.

I/S Management should provide the written responses to the Audit Management Leader and not directly to the Auditor. If I/S Management disagrees with the finding, a rebuttal should be drafted that explains why the issue should not be a finding. Otherwise, a Corrective Action Plan should be provided that outlines how the finding will be corrected and an anticipated completion date. If an I/S Management response includes a Corrective Action Plan that requires an additional Work Request to be opened, the response should be discussed with the Client Management organization that supports the steering committee under which the request will be opened.

The Audit Management Leader will review the finding and the I/S Management response against any related findings and/or responses from other recent audits to ensure that consistent replies are being provided. The Audit Management Leader will then provide feedback to the area responsible for providing the I/S Management response.

8.3.8 Remediation Planning Phase

During this phase (see Figure 8-8, next page), the Audit Management Leader consolidates the I/S Management responses into a Corrective Action Plan (CAP) that has responsible parties for each item and target completion dates. If any of the corrective actions require that another work type be opened (for example, a Work Request, Service Request, incident, etc.), this will be noted in the plan. The Audit Management Leader will ensure that the appropriate work type is initiated. The actual activity to remediate the finding will be performed following the processes for that work type.

If the remediation activity does not actually begin until after the audit is completed, the Audit Management Leader will follow up after the Audit Request is closed to ensure that the remediation activity is completed. The person providing the Corrective Action Plan should be included in the remediation activities to ensure that the remediation is performed in accordance with the Corrective Action Plan.

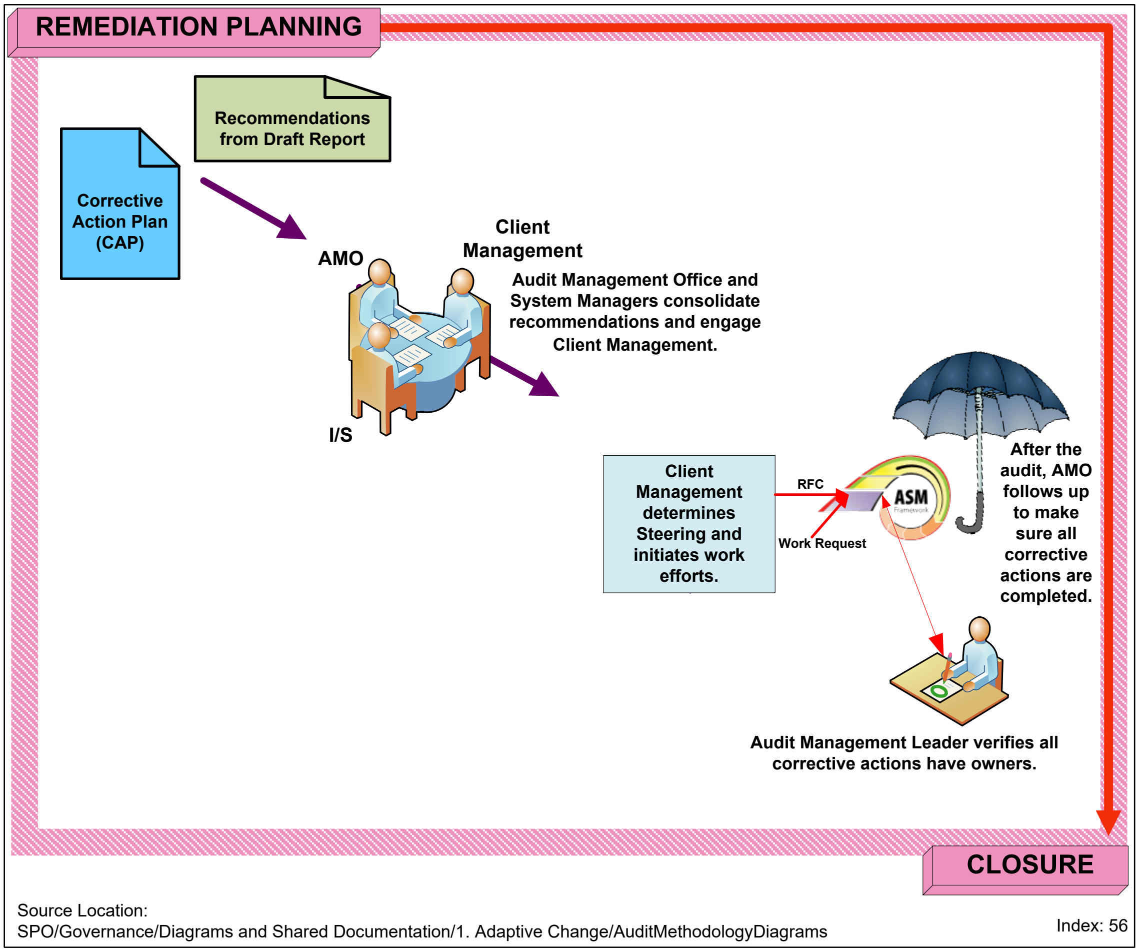

REMEDIATION PLANNING
Recommendations from Draft Report
Corrective Action Plan (CAP)
AMO
Client Management
I/S
Audit Management Office and System Managers consolidate recommendations and engage Client Management.
Client Management determines Steering and initiates work efforts.
RFC
Work Request
ASM
After the audit, AMO follows up to make sure all corrective actions are completed.
Audit Management Leader verifies all corrective actions have owners.
CLOSURE
Source Location:
SPO/Governance/Diagrams and Shared Documentation/1. Adaptive Change/AuditMethodologyDiagrams
Index: 56

Figure 8-8 Remediation Planning Phase

8.3.9 Closure

When the final audit report is received from the Auditor, the Audit Management Leader will then send it to the Direct Reports and the I/S POCs. The Audit Management Leader will request closure of the Audit Request on ***MPS*** after the remediation planning is complete and the final report has been distributed. Closure of the Audit Request is completed by Client Management as with other Work Requests.

Printed forms of this document are uncontrolled and may be obsolete. It is the responsibility of the user to ensure that any printed copy is the same revision as the online version.