HP Service Manager

for supported Windows® and Unix® operating systems

Software Version: 7.1x

Processes and Best Practices Guide

Document Release Date: July 2009
Software Release Date for SM 7.10: Dec. 2008
Software Release Date for SM 7.11: July 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Content

1 HP Service Manager Processes and Best Practices

Welcome to the HP Service Manager® Processes and Best Practices guide. HP Service Manager enables organizations to manage their IT infrastructures efficiently and effectively. This guide documents the best practice workflows that are standard with out-of-box Service Manager applications. It includes high-level workflow diagrams and step-by-step guidelines.

The Service Manager best practice workflows are based on the Information Technology Infrastructure Library (ITIL) standard, a widely recognized source of guidelines for Information Technology Service Management (ITSM).

This guide describes how Service Manager applications implement the ITIL guidelines.

Topics in this section include:

Overview of Service Manager

Service Manager is HP's enterprise service management solution. Its integrated applications are designed for out-of-box implementation, with best practice work flows that help organizations support their infrastructure and drive competitive advantage in their core businesses.

Service Manager enables companies to manage their service and support operations. It provides the tools and workflows needed to manage corporate assets: the people, knowledge, information, processes, equipment, documentation, software, and all tangible resources collectively known as *infrastructure*.

Architecture

Service Manager has a three-tiered client/server architecture:

- The presentation layer displays information to the user through a client (either a web client or Windows client). Service Manager displays information to the user on forms.
- The application layer consists of the various applications and the Run-Time Environment (RTE). The application server executes the workflow code.
- The database layer is an external relational database management system (RDBMS) to which Service Manager has been mapped. The database stores the application workflow code and the format descriptions.

An administrator sets parameters in the Service Manager initialization (sm.ini) file to select language, display color scheme of the forms, connection parameters to the relational database management system (RDBMS) and so on.

Service Manager Run-time Environment (RTE)

The foundation of the Service Manager architecture is the RTE. The RTE is the collection of executable programs that interprets the applications and translates application requests into appropriate actions for a specific platform.

RTE functions include:

- Processing application code.
- Managing the front-end graphical user interface (GUI).
- Handling database transactions.
- Accepting client connections.
- Initiating application processing.

Service Manager clients

The Service Manager clients allow users to interface with the Service Manager applications. The application server retrieves a form from the database and passes it as a client. The client interprets and builds the form and presents it to the user.

Windows client

The Windows client runs on Microsoft Windows platforms but can connect to a server running on any supported platform.

Web client

The web client runs from a web browser and connects to the web tier (a system where a supported web application server and web server are installed). The web tier in turn connects to the Service Manager server, which can run on any supported platform.

Service Manager applications

Service Manager's integrated applications are designed for ease-of-use and management of interrelated events that occur throughout the service life cycle of an asset. The core applications enable out-of-box workflow for IT Service Management (ITSM). Additional applications optimize productivity and improve cost controls. For example, Service Manager can process a reported incident through restoration of service, analysis, and, when necessary, changes to the IT infrastructure.

Overview of Service Manager best practices

To help you make optimal use of the functionality of Service Manager, HP has created best practices based on industry standard practices and on practical experience gained from Service Manager implementations with many customers of various sizes.

Service Manager applications incorporate best practice workflows in an out-of-box solution to streamline implementation. Using the out-of-box workflows results in less time designing and developing tools, and more time supporting business operations. Sample data and Service Manager Best Practice documentation provide additional guidelines for best practice implementation.

ITSM Industry Standards

Service Manager best practices are based on ITIL V3 theory. Service Manager embeds and incorporates the ITIL best practices that are used by organizations worldwide to establish and improve their capabilities in service management.

Applicable controls from Control Objectives and IT Process Framework (COBIT) 4.1 and International Organization for Standardization (ISO) 20000 are also incorporated in the processes.

- COBIT 4.1 and the Service Manager best practices describe the mapping between the COBIT 4.1 controls and the applicable Service Manager best practices reference.
- ISO 20000 and the Service Manager best practices describe the mapping between the ISO 20000 controls and the applicable Service Manager best practices reference.

By making optimal use of the functionality that Service Manager offers, you can implement state-of-the-art service management processes.

ITIL V3

ITIL processes provide a framework with which you can identify, record, and control all of the objects that make up an information technology (IT) infrastructure. It has become the most widely accepted approach to ITSM in the world. A key concept of ITIL is that of *services.* A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. ITIL V3 is a lifecyle-based approach with five stages aimed at delivering a set of services to achieve defined business outcomes.

ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organizations' growing dependency on IT and embodies best practices for IT Service Management. For complete information on ITIL, see their web site at **www.itil-officialsite.com**.

The HP Service Manager processes are based on ITIL V3 theory and are referenced in the ITIL V3 core. The ITIL core consists of the following five documents, each of which describes a different aspect of providing Service Management:

- *Service Strategy* focuses on how to design, develop, and implement Service Management both as a service and as a strategic asset. It gives guidance on how to improve the alignment between your Service Management capabilities and your business strategies. Important topics include Service Portfolio Management and Financial Management.
- *Service Design* focuses on how to design, develop, improve, and maintain value over the lifecycle of services and Service Management processes. It gives guidance on how to convert strategic objectives into services and service assets. Important topics include Availability Management, Capacity Management, Continuity Management, and Security Management.
- *Service Transition* focuses on how to transition new or updated services into operation. It gives guidance on how to control the risks of failure and disruption and prevent undesired consequences while still allowing innovation. Important topics include Change Management, Release Management, Configuration Management, and Service Knowledge Management.
- *Service Operation* focuses on the activities required to manage service operation and to achieve effectiveness in the delivery and support of services as defined in Service Level Agreements with the customers. Important topics include Incident Management, Problem Management, and Request Fulfillment.
- *Continual Service Improvement* focuses on how to create and maintain value by continual improvement to the quality of the services that an IT organization delivers to a business or customer. Important topics include Service Reporting, Service Measurement, and Service Level Management.

Service Manager best practices implement the following processes found in the ITIL *Service Transition* and *Service Operation* documents. These processes are described in the chapters that follow.

Table 1-1 ITIL processes referred to in this document

ITIL V3 Core Volume	ITIL Chapter Name	SM Process ID
Service Operations	Incident Management	SO 2
Service Operations	Problem Management	SO 4
Service Transition	Change Management	ST 2
Service Transition	Configuration Management	ST 3

ISO 20000

ISO/IEC 20000 consists of two parts under the general title, Information Technology Service Management: Code of practice ISO 20000-1. The subject of Part 1 “promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirements.”

It comprises ten sections:

1 Scope

2 Terms and Definitions

3 Requirements for a Management System

4 Planning and Implementing Service Management

5 Planning and Implementing New or Changed Services

6 Service Delivery Process

7 Relationship Processes

8 Control Processes

9 Resolution Processes

10 Release Process

ISO 20000-2 is a “Code of Practice” and describes the recommendations for service management within the scope of ISO 20000-1. It comprises the same sections as Part 1 except that it excludes the Requirements for a Management System as no requirements are imposed by Part 2. Service Manager’s best practices coverage of the ISO 20000-2 code of practice items is shown in Service Manager’s compliance with ISO 20000 on page 233.

COBIT 4.1

COBIT (the Control Objectives for Information and related Technology) was developed by the IT Governance Institute (**www.ITGI.org**) to advance international thinking and standards in directing and controlling enterprise information technology. COBIT supports IT Governance through its framework of 34 IT processes. This framework ensures business and IT alignment, maximizes IT enablement of business processes, optimizes IT resources, and manages risk.

COBIT groups its 34 processes into four domains:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Each process has a high-level control objective (the desired outcome) and one or more detailed control objectives that address the requirements of the actual activities that it performs.

COBIT ensures:

- IT and business alignment
- IT enabled business processes
- IT resource optimization
- IT management of risks

COBIT's framework accomplishes these goals by focusing on the business requirement for information, and the structured (process) utilization of IT resources. COBIT's framework establishes what needs to be done to provide the information the enterprise needs to achieve its goals. IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

These requirements:

- Provide statements of managerial actions to increase value or reduce risk
- Consist of policies, procedures, practices and organizational structures
- Provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

Service Manager's best practices coverage of COBIT is shown in Service Manager's compliance with COBIT 4.1 on page 237.

Service Management organization

The Service Manager best practices include processes, user role descriptions involved in each process, and task flows for each service management area. The process can meet best practices when employees involved in the process are assigned user roles in your IT organization.

Most of the distinct process roles are assigned according to the applicable support group. The service desk is its own support group and has specific user roles that are assigned to the employees within your IT organization. All other support groups (for example, second- and third-line support and suppliers) should have a similar set of process roles assigned.

Organizational model and user roles

To ensure that all user actions and responsibilities can be easily assigned to individual users or to user groups, each HP Service Manager process is included in a detailed organizational model with well-defined user role descriptions, activity types, and responsibilities. To use the Service Manager organizational model within your organization's specific IT environment, first assign each process role to the appropriate personnel. The Service Manager organizational model provides the following process areas, each with defined user roles.

The responsibilities related to each of these roles are located these sections:

- User Interaction Management user roles on page 28
- Incident Management user roles on page 57
- Problem Management user roles on page 98
- Change Management user roles on page 154
- Configuration Management user roles on page 197

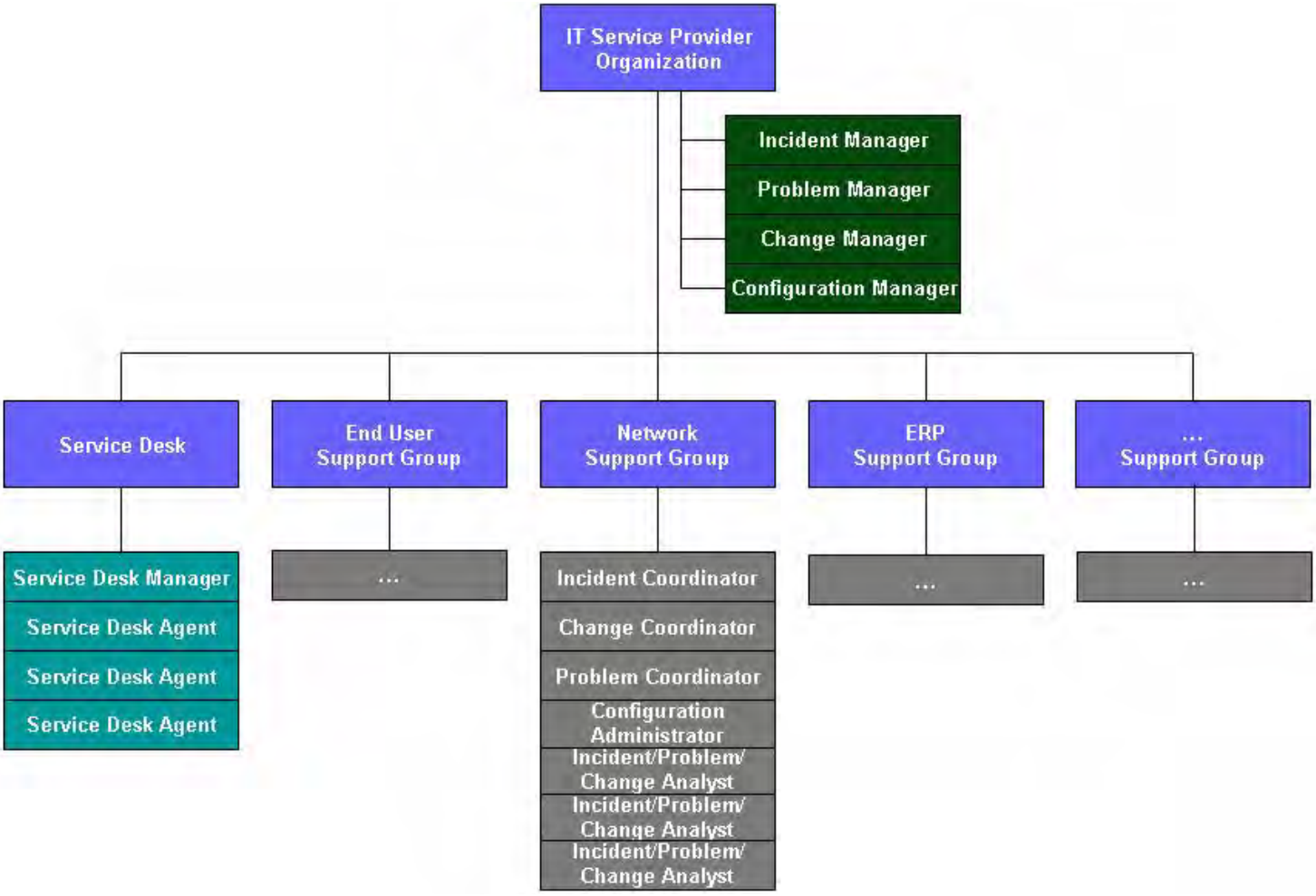

Figure 1-1 Example of an IT Organization

Service Manager best practice processes

The Service Manager process flow in Figure 1-2 on page 19 describes the ITSM processes implemented in the following applications:

- *Service Desk* — The Service Desk application includes all direct interaction between a user and the service desk by phone or by email. It also includes all user activities that occur by use of the self-service Web portal (for example, searching the knowledgebase, checking for status updates, or logging an interaction). For more information on this application and the associated processes, go to Chapter 2, User Interaction Management Overview.
- *Incident Management* — The Incident Management application ensures that incidents are resolved within agreed-on service level targets and automates reporting and tracking of a single incident or a group of incidents associated with a business enterprise. It also enables you to categorize and track various types of incidents (such as service unavailability or performance issues, hardware or software failures, etc.) and to track the resolution of these incidents. For more information on this application and the associated processes, go to Chapter 5, Incident Management Overview.
- *Problem Management* — The Problem Management application helps to minimize the effects of incidents caused by errors in the IT infrastructure and to prevent their recurrence by enabling you to identify the underlying reason for one or more incidents, implement workarounds, identify known errors, and provide permanent solutions. Its purpose is to prevent problems and resulting incidents, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented. For more information on this application and the associated processes, go to Chapter 8, Problem Management Overview.

Incident Management and Problem Management are separate processes although they are closely linked. Incident Management expressly covers the restoration of services to users, whereas Problem Management covers identifying and removing the causes of incidents.

- *Change Management* — The Change Management application controls the process to request, manage, approve, and control changes that modify your organization's IT infrastructure. This process includes changes to all assets and configuration items, such as network environments, facilities, telephony, and resources. It covers changes to baseline service assets and configuration items across the entire service life cycle. For more information on this application and the associated processes, go to Chapter 13, Change Management Details.
- *Configuration Management* — The Configuration Management application ensures that selected components of a complete IT service, system, or product (the Configuration Item) are identified, baselined, and maintained and that changes to them are controlled. It also ensures that releases into controlled environments and operational use are completed on the basis of formal approvals. For more information on this application and the associated processes, go to Chapter 14, Configuration Management Overview.

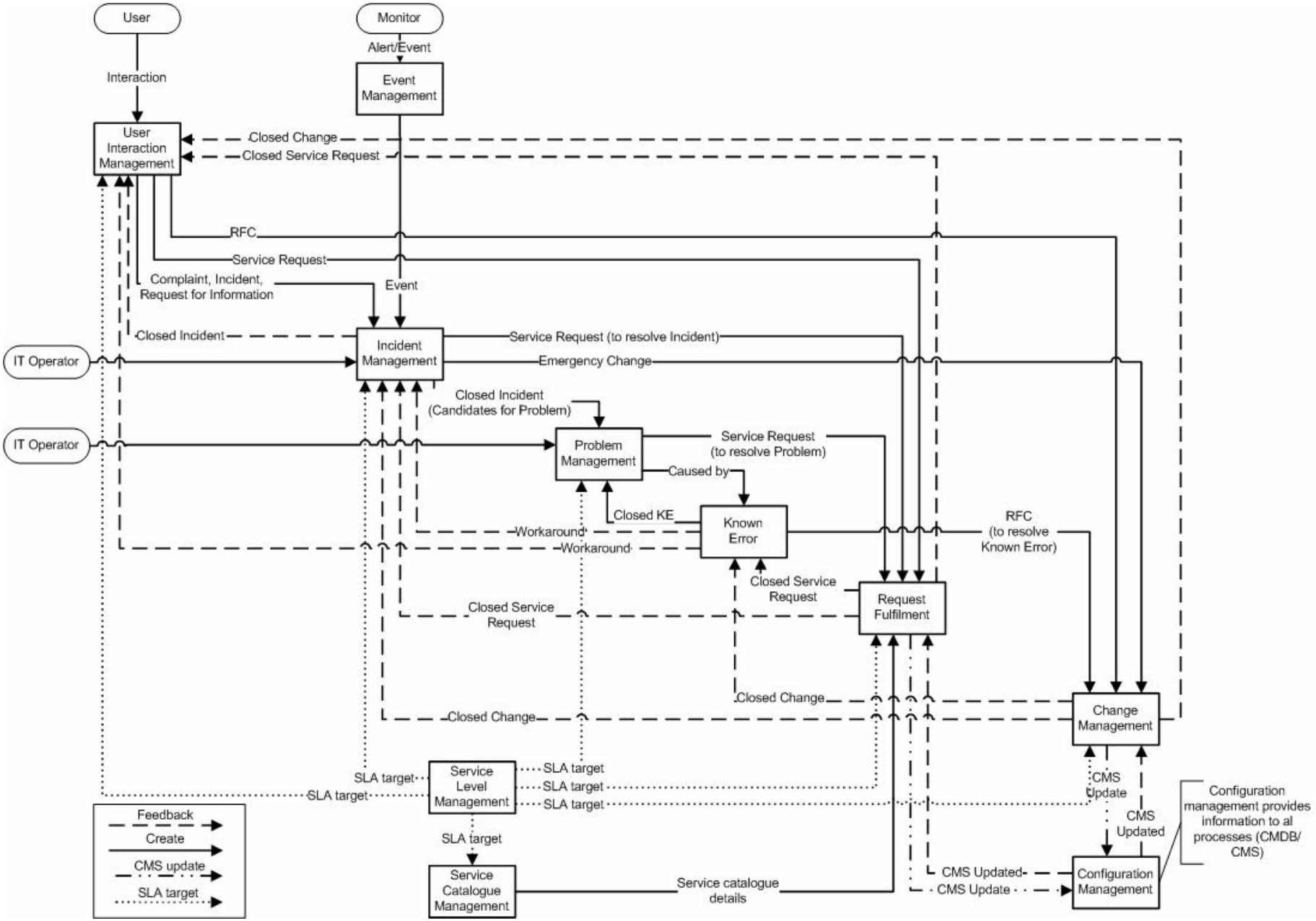

Figure 1-2 Service Manager process flow chart

Relationships between Service Manager applications

Each Service Manager application interacts closely with several others and supports several service management processes.

Service Desk

Many incidents start as issues communicated by end users to the service desk. When a Service Desk Agent cannot resolve and close an issue on first contact, he or she escalates it to an incident. If the Service Desk Agent finds an existing incident that affected the same CI or one of the related CI's, the incident is associated with the interaction record. If an existing incident ticket is not found, a new incident ticket is opened, based on the Service Desk interaction. When the incident is resolved and closed, the Service Desk communicates the closure to the end user and closes the interaction that initiated the incident. If the reason for a call is a disruption in service and the Service Desk Agent cannot resolve the issue, it is escalated to Incident Management until service is restored.

Incident Management

Incident Management provides effective incident classification and tracking to provide good data for analysis. The Knowledge Base that Service Manager builds and maintains is a solution repository for new incidents. Matching incidents to problems and known errors is the first step in spotting trends. Subsequently, trend analysis helps you remove errors before they affect a large segment of users. As part of the Incident Investigation and Diagnosis process, an Incident Analyst can open new emergency changes required for immediate resolution of the incident. This is only the case if there is no effective or useful workaround available.

In the Emergency Change Handling process, the Change Analyst informs the Incident Manager about successfully implemented emergency changes and, if the Incident Manager agrees, closes the related incident ticket.

Incident Management contributes to improved service levels.When an incident is opened, the default Base Monitoring Service Level Agreement (SLA) for IT services is triggered. This SLA specifies response objectives (the maximum time allowed before an incident should reach the resolved state), but does not define availability objectives. Both problems and incidents affect service delivery.

Problem Management

Incident Management forms part of the overall process of dealing with problems in the organization. Incidents are often caused by underlying problems that must be solved to prevent the incident from recurring. Service Manager allows you to enable certain Incident Management users to indicate problem candidates. The incident ticket includes a field that indicates whether the issue that caused the incident is most likely a problem and should have a problem ticket created for it. In addition, as part of the Incident Investigation and Diagnosis process, the operator needs to consider whether the incident is related to an open problem or known error. If it is, they must relate the incident ticket to the problem ticket or known error record. The incident then remains open until a workaround for the problem becomes available. If related to a known error, there will always be a workaround.

Problem Management maintains information about problems and the appropriate workarounds and resolutions, which helps an organization reduce the number and impact of incidents over time. Problem Management has a strong interface with Knowledge Management, and tools such as the Known Error Database are used for both. This gives operators the ability to search the knowledgebase for useful

information and to contribute to it, benefiting those who are investigating, diagnosing, and resolving incidents and interactions. Incident Management operators can search the knowledgebase, and can create a knowledge article based on the incident at hand.

Change Management

Service Desk open-idle interactions with a category of Request for Change can be escalated to Change Management. These change requests are reviewed by a Change Coordinator who either assigns the change to the applicable support group to make it part of the Change Review process, or rejects the change request. Changes rejected for insufficient information are returned to the Service Desk Agent for additional information gathering. Others are rejected because the change is no longer valid.

When operators determine that an incident was caused by a change, they search the Changes database to see if a recent change may have caused the service disruption. If such a change exists, they can link the two records. If no such change exists, but a new change should be registered, they can open a new change. The operator can also look at any changes that have recently been performed against the reported Configuration Item.

Problem Management submits resolutions and workarounds that require a change to Change Management. Change Management tracks and implements the Request for Change (RFC), which permanently changes the infrastructure and prevents future incidents. When the RFC is complete, the Problem Management process reviews the change before the known error record can close.

An integration to HP Universal CMDB adds and updates configuration item (CI) records that can trigger an unplanned change or change verification action in Change Management. If the integration detects updates to a CI that do not match an existing change request, Service Manager creates a new change request with the unplanned change category. A Change Coordinator can then review the change and approve or deny it. If the integration finds a matching change request, it can verify the CI attributes against the expected values and automatically close the change if they match.

Configuration Management

Configuration Management is used throughout the system to help identify and track configuration items (CIs) as necessary. Accurate tracking of incidents and changes starts with control of resources and their relationships. For example, when operators escalate an interaction or open an incident directly, they may specify the affected configuration item. When a configuration item is identified, the Incident Management process investigates and attempts to resolve the issue with the item. The final resolution may require a problem ticket to be created to fix the source of the problem, and generate change request in Change Management. Scheduled maintenance uses configuration management to enables the automatic creation of Incident tickets and Change requests for regular proactive maintenance. The Incident Analyst can also view the Configuration Item tree to discover if related Configuration Items could have caused the incident.

2 User Interaction Management Overview

The HP Service Manager Service Desk application, referred to as Service Desk throughout this chapter, supports the service desk function of the Information Technology Infrastructure Library (ITIL) with its User Interaction Management processes for the IT service and the customer base. The Service Desk application provides a single point of entry to the other Service Manager applications and enables you to document and track all calls received by the service desk.

Service Desk incorporates the essential concepts of ITIL to ensure that the best practices of IT service management are applied to the service desk to aid end customers, ensure data integrity, and streamline communication channels in the organization.

This section describes how Service Desk implements the best practice guidelines for the User Interaction Management processes.

Topics in this section include:

The service desk within the ITIL framework

Service Operation is one of five core publications from ITIL that covers the service lifecycle. The purpose of service operation is to deliver agreed-on levels of service to users and customers, and to manage the applications, technology, and infrastructure that support delivery of the services.

The *service desk* is a key function of service operation. It provides a single, central point of contact for all users of IT. The service desk's goal is to restore normal service to users as quickly as possible. Restoring normal service could involve fixing a technical fault, fulfilling a service request, or answering a query — whatever is needed to enable users to return to their work. The service desk logs and manages customer interactions and provides an interface to other service operation processes and activities.

ITIL V3 notes these specific responsibilities of a service desk:

- Logging, categorizing, and prioritizing all calls
- Providing first-line investigation and problem diagnosis
- Resolving incidents or service requests to be handled at the service desk level
- Escalating incidents and service requests that cannot be resolved within agreed-on time limits
- Closing resolved incidents, requests, and other calls
- Communicating with users to keep them informed of progress, impending changes, agreed-on outages, and other such notifications.

The Service Desk application

The HP Service Manager Service Desk application incorporates the ITIL best practices that are used by organizations worldwide to establish and improve their capabilities in service management.

It provides a central *Service Operation* function, coordinating the efficient and effective delivery of services to end users and enabling various improvements, including the following:

- Improved customer service and satisfaction
- Increased accessibility through a single point of contact and information
- Better quality and faster turnaround of customer or user requests
- Improved teamwork and communication
- Enhanced focus and a proactive approach to service provision
- Improved usage of IT resources and increased productivity of all users

The Service Desk application enables a Service Desk agent to document and track user interactions. Service Desk provides one-click access to other Service Manager applications to automatically enter information received.

The Service Desk application covers:

- Direct interactions between a user and the service desk by phone or by email
- User activities that occur from use of the self-service Web portal (for example, searching the knowledgebase, checking for status updates, or logging an interaction).

One of the best practices that derives from ITIL's service desk function is that user interactions should not be saved and updated later. Therefore, the Service Desk application requires that any new interaction either be resolved within the agreed upon time limits and then closed or, if it cannot be resolved, escalated. The information gathered during the customer interaction can be used to open an incident ticket if a reported issue requires further action. It can also be added to a record in another Service Manager application, such as Change Management.

User Interaction Management process overview

Every user contact with the service desk is logged as an interaction. User Interaction Management is the process for handling all interactions with the service desk that are received from self-service Web pages or directly by service desk personnel. These interactions can include service disruptions, service requests, requests for information (RFI), or complaints reported by users who communicate with the service desk by using instant messages, phone, email, or by self-service Web pages. The User Interaction Management process enables you to easily log and resolve simple user requests and to escalate others into incidents requiring further action.

Multiple user interactions can be linked to a single incident ticket in the tool. User Interaction Management describes all the activities a Service Desk agent needs to follow when registering a new incident or change. The Service Desk agent follows the necessary steps and searches for related knowledge records, known error records, and existing incidents or changes. This process streamlines service desk activities, thereby decreasing the workload for second line support teams.

A general overview of the User Interaction Management processes and workflows is depicted in Figure 2-1,below. They are described in detail in Chapter 3, User Interaction Management Workflows.

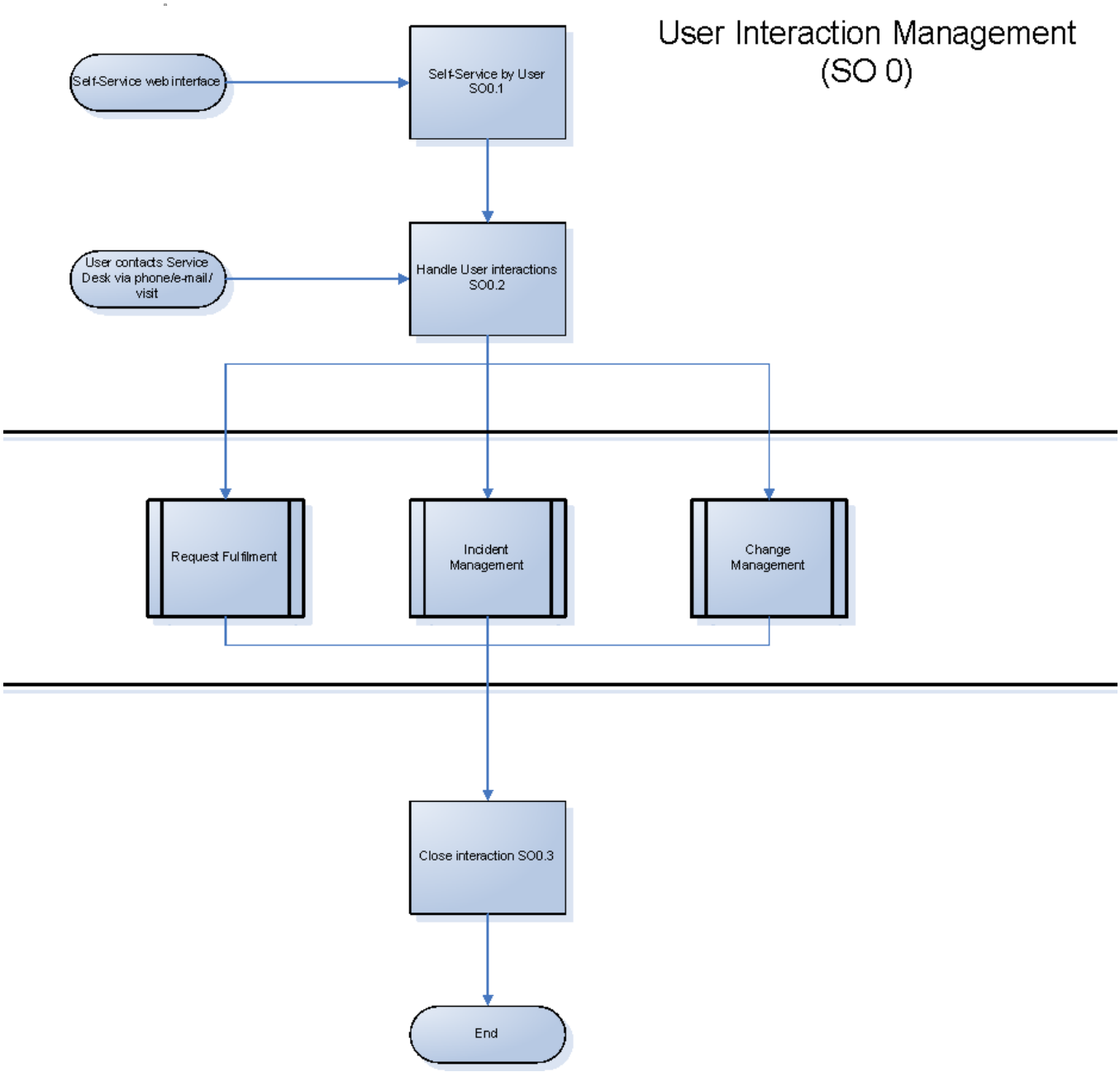

Figure 2-1 User Interaction Management process diagram

When a user contacts the service desk, the Service Desk agent uses the Service Desk application to create an interaction record. The Service Desk agent records the user name, the name of the component that the user is calling about, and a description of the service request. After collecting this information, the Service Desk agent performs the actions required to resolve the user request.

- If the service request is resolved without escalating it to an incident, the Service Desk agent can close the interaction record.
- If the service request cannot be resolved without escalating it to an incident, the Service Desk agent searches for existing incidents that affect the same component or one of the parent assets of that component.
  - If an existing incident is found, the Service Desk agent can associate the current interaction with the existing incident ticket.
  - If an existing incident ticket is not found, the Service Desk agent can register a new incident based on the Service Desk interaction. Service Desk copies information from the interaction record into the newly-created incident ticket.

For example, consider a user who cannot print to a network printer:

1. The user contacts the service desk for assistance.
2. The Service Desk agent populates an interaction record with the relevant information.
3. Because the issue cannot be resolved immediately, the Service Desk agent opens an incident, and the incident is assigned to a technician.
4. The technician discovers that the printer network connection is broken.
5. The technician fixes the connection and closes the incident.
6. The Service Desk agent contacts the user and instructs the user to attempt printing to the network printer.
7. If the user can successfully print, the Service Desk agent can close the interaction. If the user still cannot print, the Service Desk agent may reopen the existing related incident ticket or create a new incident and then relate the unsolved interaction.
8. If the user wishes to report a related or new issue, the Service Desk agent closes the interaction (as the original issue was resolved) and opens a new interaction detailing the new issue the user needs to report.

User Interaction Management user roles

Table 2-1 describes the responsibilities of the User Interaction Management user roles.

Table 2-1 User Interaction Management user roles

Role	Responsibilities
User	• Report all IT-related requests to the service desk or use the self-service Web pages. • Validate solutions and answers provided by the IT department to a registered service request.
Service Desk Agent	• Register interactions based on contact with user. • Match user interaction to incidents, problems, known errors, or knowledge document. • Solve and close interactions. • Provide status updates to users on request. • Register incident based on a user interaction and assign to the correct support group. • Register Request for Change, based on a user interaction. • Register Service Request, based on a user interaction. • Validate a solution provided by a support group. • Report and verify a solution to a user. • Monitor Service Level Agreement (SLA) targets of all incidents registered and escalate, if required. • Communicate about service outages to all users.

Input and output for User Interaction Management

Interactions can be triggered and resolved in several ways. Table 2-2 outlines the inputs and outputs for the User Interaction Management process.

Table 2-2 Input and output for User Interaction Management

Input to User Interaction Management	Output from User Interaction Management
A user can contact the service desk and give input by using instant messages, phone, email, self-service web pages, or other means.	Service desk personnel can handle an interaction in the following ways: • If the interaction is related to a new or existing incident, the interaction is handled by using the Incident Management process. • If the interaction involves a request, the interaction is sent to the request fulfillment process. • If the interaction requires a change, the interaction is sent to the Change Management process.

Key performance indicators for User Interaction Management

The Key Performance Indicators (KPIs) in Table 2-3 are useful for evaluating your User Interaction Management processes. To visualize trend information, it is useful to graph KPI data periodically. In addition to the data provided by Service Manager, you may need additional tools to report on all of your KPI requirements.

Table 2-3 Key Performance Indicators for User Interaction Management

Title	Description
First time fix	Percentage of interactions closed by the Service Desk agent at first contact without reference to other levels of support
First line fix	Percentage of interactions closed by the service desk without reference to other levels of support
Customer satisfaction	Customer satisfaction measured by surveys completed by customers

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included below.

ITIL V3 Key Performance Indicators

The following are ITIL V3 KPIs for User Interaction Management:

- Percentage of incidents closed by the service desk without reference to other levels of support (that is, closed by first point of contact).
- Number and percentage of incidents processed by each Service Desk agent.

COBIT 4.1 Key Performance Indicators

The following are the COBIT 4.1 KPIs for User Interaction Management:

- Amount of user satisfaction with first-line support (service desk or knowledgebase)
- Percent of first-line resolutions based on total number of requests
- Call-abandonment rate
- Average speed to respond to telephone and email or Web requests
- Percent of incidents and service requests reported and logged using automated tools
- Number of days of training per service desk staff member per year
- Number of calls handled per service staff member per hour
- Number of unresolved queries

RACI matrix for User Interaction Management

A Responsible, Accountable, Consulted, and Informed (RACI) diagram or RACI matrix is used to describe the roles and responsibilities of various teams or people in delivering a project or operating a process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. The RACI matrix for User Interaction Management is shown in Table 2-4.

Table 2-4 RACI matrix for User Interaction Management

Process ID	Activity	User	Service Desk Agent	Service Desk Manager
SO 0.1	Self-Service by User	R	I	A
SO 0.2	Interaction Handling	R	R	A
SO 0.3	Interaction Closure	R/I	R	A

3 User Interaction Management Workflows

Every time a user contacts the service desk it is logged as an interaction. User interaction management is the process of handling all interactions with the service desk that are received from self-service Web pages or directly by service desk personnel. These interactions can include service disruptions, service requests, requests for information (RFI), and complaints reported by users who communicate with the service desk by using instant messages, phone, email, or self-service Web pages.

The Service Desk agent follows the necessary steps and searches for related knowledge records, known error records, and existing incidents or changes. The process enables Service Desk agents to easily log and resolve simple user requests and to escalate others into incidents requiring further action. The process streamlines service desk activities and decreases the workload for second-line support teams.

The User Interaction Management process consists of the following processes, which are included in this chapter:

Self-Service by User (process SO 0.1)

By using the self-service web environment, users can perform the following activities without contacting the service desk:

- Search the knowledgebase to find an answer to a question or issue
- Monitor the status of previously reported interactions
- Log new interactions
- Order items from the service catalog

You can see the details of this process in the following figure and table.

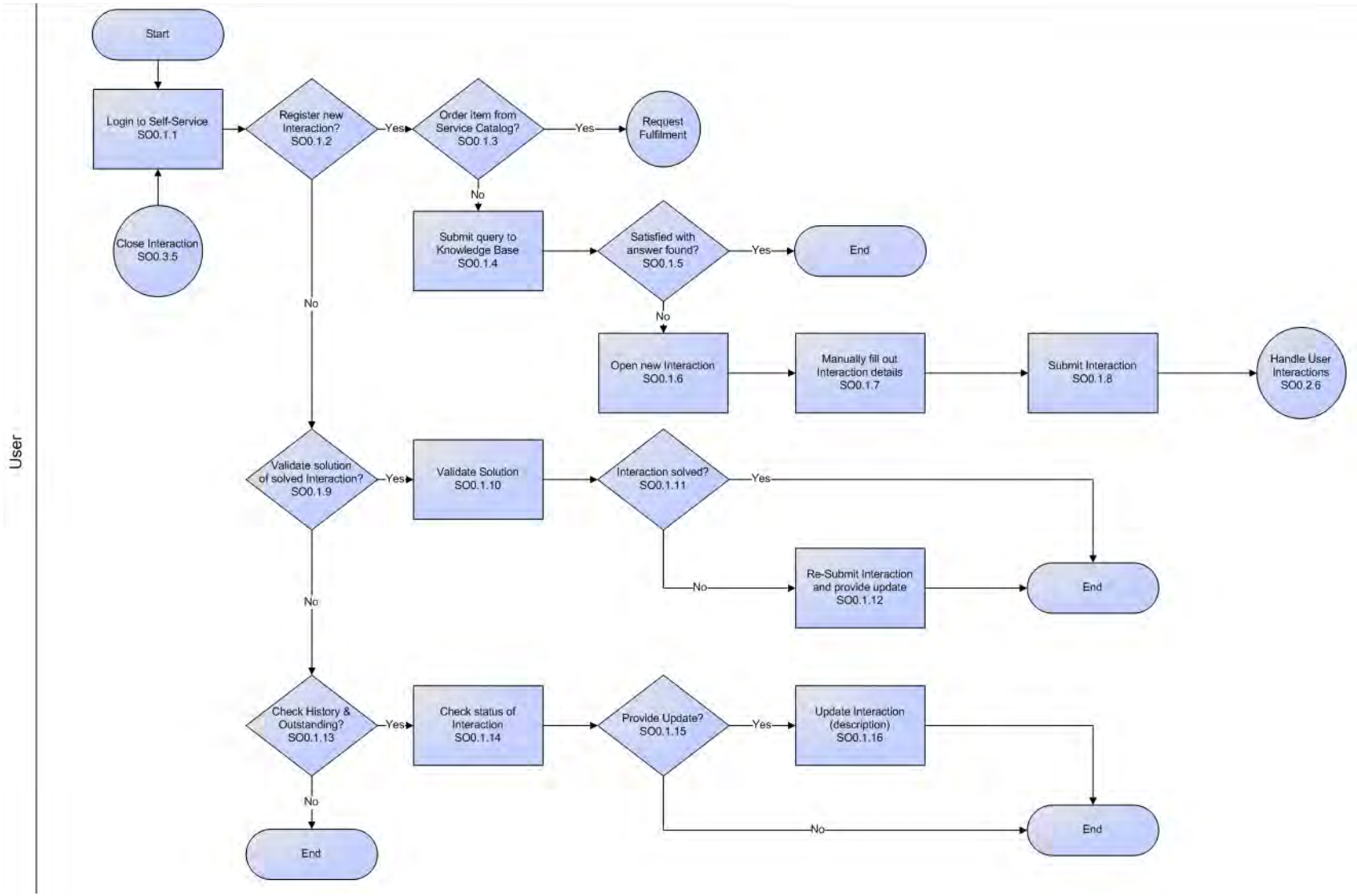

Figure 3-1 Self-Service by User (SO 0.1)

Table 3-1 Self-Service by User (SO 0.1) process

Process ID	Procedure or Decision	Description	Role
SO 0.1.1	Log in to Self-Service	To gain access to the Self-Service Web interface, users must log on by using their login credentials.	User
SO 0.1.2	Register new interaction?	If yes, continue with SO 0.1.3. If no, go to SO 0.1.9.	User
SO 0.1.3	Order item from service catalog?	If yes, go to the request fulfillment process. If no, submit a query to the KnowledgeBase.	User
SO 0.1.4	Submit query to knowledgebase	To search for a knowledge document, users must complete a search.	User
SO 0.1.5	Satisfied with answer found?	If yes, stop. If no, go to SO 0.1.6.	User
SO 0.1.6	Open a new interaction	To open a new interaction from the knowledge search screen, users must click the New Interaction button.	User
SO 0.1.7	Manually complete interaction details	To register a new interaction, users must provide a description of the request; select the urgency, affected Service, and preferred contact method; and can optionally add an attachment.	User
SO 0.1.8	Submit interaction	When all mandatory fields are completed, click Submit to send the request to the service desk.	User
SO 0.1.9	Validate solution of solved interaction?	To validate the solution to a previously reported interaction, go to SO 0.1.10. If no, go to SO 0.1.13.	User
SO 0.1.10	Validate solution	Use View Open Requests to get an overview of all solved interactions. Select the applicable interaction and validate the solution provided.	User
SO 0.1.11	Interaction solved?	If yes, stop. If no, go to SO 0.1.12.	User
SO 0.1.12	Resubmit interaction and provide update	When a user disagrees with the proposed solution, the user can resubmit the interaction and provide a reason for the disagreement. The newly-created interaction is automatically linked to the old interaction and sent to the service desk for further diagnosis.	User
SO 0.1.13	Check history and outstanding interactions?	If a user wants to check the status or history of previously registered interactions, go to SO 0.1.14. If no, stop.	User

Table 3-1 Self-Service by User (SO 0.1) process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 0.1.14	Check status of interaction	Use View Open Requests to get an overview of all open or closed interactions. Select the interaction and view the status with last updates.	User
SO 0.1.15	Provide update?	If a user has additional details to add to the previously-logged interaction that may be useful to know for the specialist, go to SO 0.1.16. If no, stop.	User
SO 0.1.16	Update interaction	There are two scenarios to update an interaction and have a Save button to save the updated information. • The Save button appears when a self-service user selects the option View Open Requests, selects an interaction, and clicks the Update button. Once the information is updated, the self-service user clicks Save to save the updated information in the request. • When you escalate an interaction, you can go back to the interaction to add more information or perform changes to it. You then have a Save button when you select an existing interaction. The interaction is also a status of Open - Linked or Open - Callback. Once you have added more information to the request or performed the changes, you can click Save.	User

Interaction Handling (process SO 0.2)

The service desk is responsible for handling all user interactions received by the self-service Web portal, email, or phone. The service desk attempts to resolve an interaction when the user makes first contact with the service desk. Interaction Handling includes the registration and preliminary investigation of interactions including the matching against open incidents, problems, known errors, and the knowledgebase to maximize the first-line solving ratio.

When the service desk cannot close an interaction on first contact, the Service Desk agent escalates it to Incident Management, Change Management, or request fulfilment.

You can see the details of this process in the following figure and table.

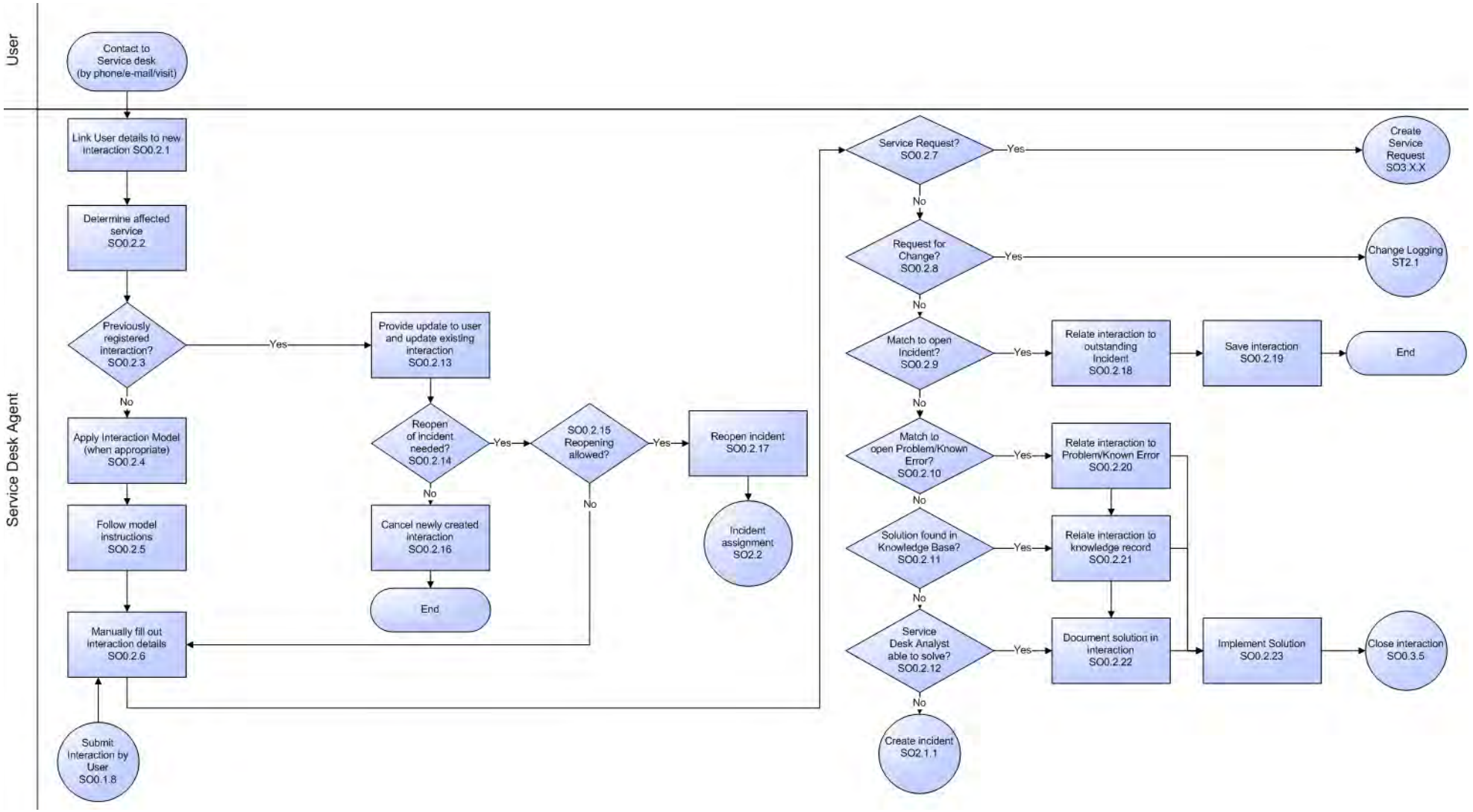

Figure 3-2 Interaction Handling (SO 0.2)

Table 3-2 Interaction Handling (SO 0.2) process

Process ID	Procedure or Decision	Description	Role
SO 0.2.1	Link user details to new interaction	Fill in the name of the caller in the Contact Person field and the name of the user in the Service Recipient field (if different).	Service Desk Agent
SO 0.2.2	Determine affected service	In the Affected Service field, select the service that matches the user request.	Service Desk Agent
SO 0.2.3	Concerns previously registered interaction?	If the user contacts the service desk for a previously registered interaction, go to SO 0.2.13. If not, go to SO 0.2.4.	Service Desk Agent
SO 0.2.4	Apply interaction model (when appropriate)	If there is an interaction model available, apply the model to quickly define the interaction. If no model exists, the default interaction settings are shown.	Service Desk Agent
SO 0.2.5	Follow model instructions	The predefined fields are filled in from the model. When there is a script attached to the model, follow the questions and fill in the answers.	Service Desk Agent
SO 0.2.6	Manually fill out interaction details	Fill out the required interaction details such as short title, a full description, interaction type, and categorization. In addition, select the applicable impact and urgency. The assignment group is automatically filled in, based on the service and categorization selected.	Service Desk Agent
SO 0.2.7	Service request?	If the interaction concerns a Service Request, go to the Request Fulfilment process. If not, go to SO 0.2.8.	Service Desk Agent
SO 0.2.8	Request for change?	If the interaction concerns a Request for Change, go to the Change process. If not, go to SO 0.2.9.	Service Desk Agent
SO 0.2.9	Match to open incident?	Based on the service and categorization, the Service Desk agent performs a search to find any open incidents that match the user interaction. If yes, go to SO 0.2.18. If not, go to SO 0.2.10.	Service Desk Agent
SO 0.2.10	Match to open problem or known error?	Based on the service and categorization, the Service Desk agent performs a search to find any open problems or known errors that match the user interaction. If yes, go to SO 0.2.20. If no, go to SO 0.2.11.	Service Desk Agent
SO 0.2.11	Solution found in knowledgebase?	Based on the description and categorization, the Service Desk agent performs a knowledgebase search. If yes, go to SO 0.2.21. If no, go to SO 0.2.12.	Service Desk Agent
SO 0.2.12	Service Desk Agent able to solve?	If the Service Desk Agent is sufficiently equipped with tools and knowledge to solve the interaction for the user, go to SO 0.2.22. If not, go to the Create Incident process.	Service Desk Agent
SO 0.2.13	Provide update to user and update existing interaction	Inform the user of recent updates made by Analysts, and then update the interaction by stating that the user requested an update.	Service Desk Agent
SO 0.2.14	Reopen incident?	If the user is unhappy with a solution provided and the incident must be reopened, go to SO 0.2.15. If not, go to SO 0.2.16.	Service Desk Agent
SO 0.2.15	Reopening allowed?	If reopening the incident is allowed due to a user request during the period of two weeks after solution notification, go to SO 0.2.17. If not, go to SO 0.2.6.	Service Desk Agent

Table 3-2 Interaction Handling (SO 0.2) process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 0.2.16	Cancel newly created interaction	Cancel the newly created interaction, as this registration is not needed anymore.	Service Desk Agent
SO 0.2.17	Reopen incident	Reopen the previously registered incident that was solved incorrectly by changing the status to Open and providing an update that states the reason that the incident was reopened.	Service Desk Agent
SO 0.2.18	Relate interaction to outstanding incident	Relate the interaction to the open incident.	Service Desk Agent
SO 0.2.19	Save interaction	Save the interaction in the interaction database and provide the interaction number to the user. There is one scenario where you have a Save button to save an interaction record. When you escalate an interaction, you can go back to the interaction to add more information or perform changes to it. You then have a Save button when you select an existing interaction. The interaction is also a status of Open - Linked or Open - Callback. Once you have added more information to the request or performed the changes, you can click Save.	Service Desk Agent
SO 0.2.20	Relate interaction to problem/known error	Relate the interaction to the problem or known error.	Service Desk Agent
SO 0.2.21	Relate interaction to knowledge record	Relate the interaction to the knowledge record to populate the solution in the interaction record.	Service Desk Agent
SO 0.2.22	Document solution in interaction	Describe the solution in the Solution field.	Service Desk Agent
SO 0.2.23	Implement solution	Perform the actions needed to implement the solution and go to the Interaction Closure process.	Service Desk Agent

Interaction Closure (process SO 0.3)

When an interaction is resolved by the Service Desk on first intake, or solved by a related incident, change, or request that is resolved, the interaction is closed. Based on user preferences, the Service Desk communicates the solution to the user by phone or email.

You can see the details of this process in the following figure and table.

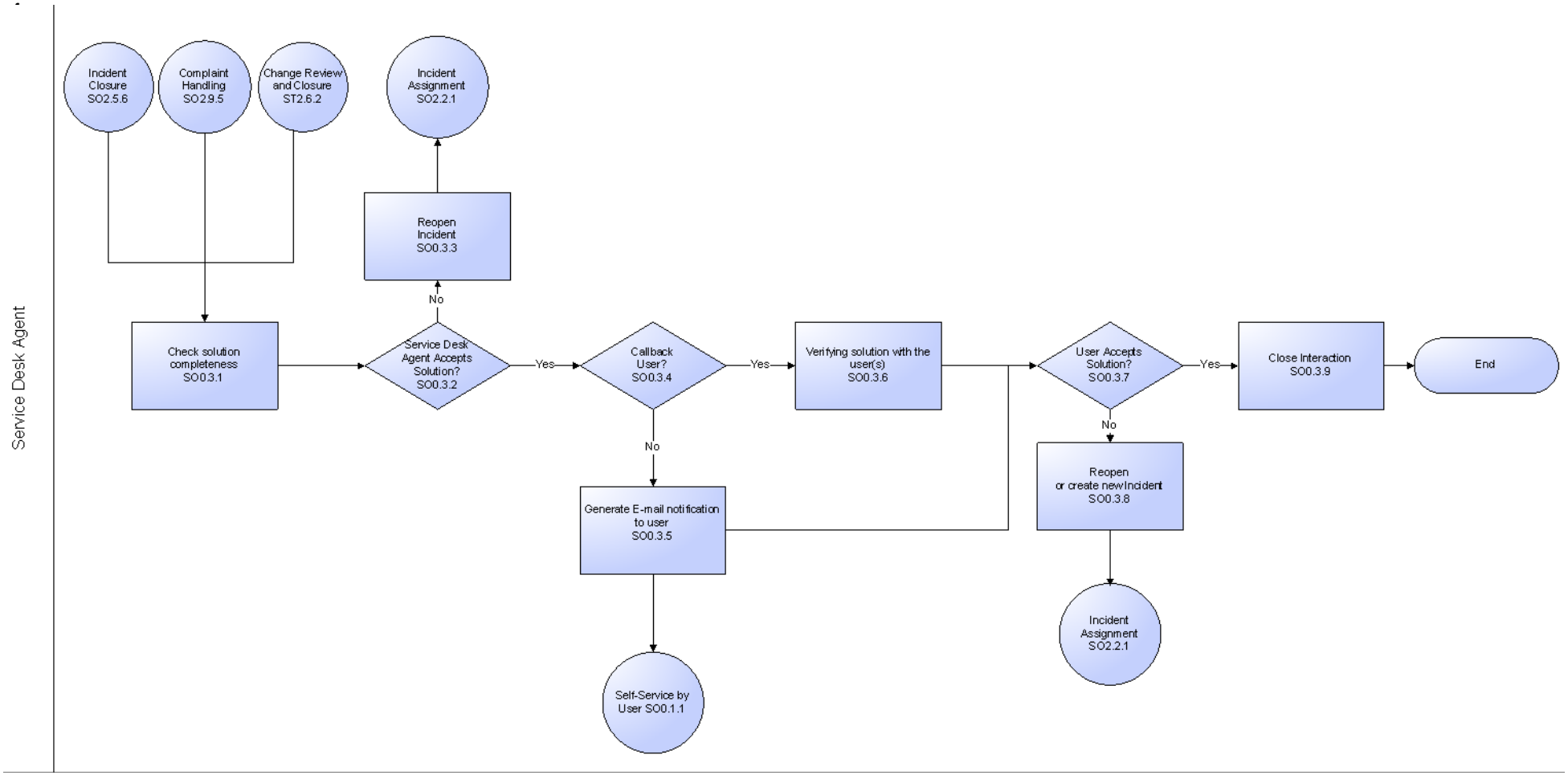

Figure 3-3 Interaction Closure (SO 0.3)

Table 3-3 Interaction Closure (SO 0.3) process

Process ID	Procedure or Decision	Description	Role
SO 0.3.1	Check solution completeness	The Service Desk agent checks the solution provided for all Open-Callback interactions.	Service Desk Agent
SO 0.3.2	Service Desk Agent accepts solution?	If yes, go to SO 0.3.4. If no, go to SO 0.3.3.	Service Desk Agent
SO 0.3.3	Reopen incident	The Service Desk agent reopens the incident ticket for further investigation and diagnosis.	Service Desk Agent
SO 0.3.4	Call back user?	If the Notify By method states that the user wants to be notified by phone, go to SO 0.3.6. If not, go to SO 0.3.5.	Service Desk Agent
SO 0.3.5	Generate email notification to user	The user receives an automatic email about the interaction closure containing the interaction details, including the solution. The user can check the solution by using the self-service Web portal, and can reject the solution within two weeks. After two weeks, the interaction is automatically closed.	Service Desk Agent
SO 0.3.6	Verify solution with the user	The Service Desk Agent contacts the user and communicates the resolution. The user should verify the solution and confirm that the incident is solved and that the question or complaint is answered, or the Service Request is fulfilled.	Service Desk Agent
SO 0.3.7	User accepts solution?	If yes, go the SO 0.3.9. If no, go to SO 0.3.8.	Service Desk Agent
SO 0.3.8	Reopen or recreate incident	The solution provided may not solve the issue for all users. If the solution does not solve the issue for all users, the Service Desk Agent must either reopen the existing incident or create a new incident, and then relate the unsolved interaction(s).	Service Desk Agent
SO 0.3.9	Close interaction	The Service Desk Agent closes the interaction.	Service Desk Agent

4 User Interaction Management Details

HP Service Manager uses its Service Desk application to enable the User Interaction Management process. The main function of User Interaction Management is to monitor, track, and record calls and open incidents, as necessary.

In User Interaction Management, a Service Desk Agent receives a call and opens a new interaction. The Service Desk Agent fills in the required fields, and then chooses to close the interaction or escalate it to an incident.

This section describes selected User Interaction Management fields in the out-of-box Service Manager system.

Topics in this section include:

New interaction form

When a Service Desk Agent clicks Register a New Interaction, Service Desk displays the new interaction form. The required fields in this form must be populated to register the new interaction. Service Desk fills in some of the fields automatically. The Service Desk Agent must fill in the others.

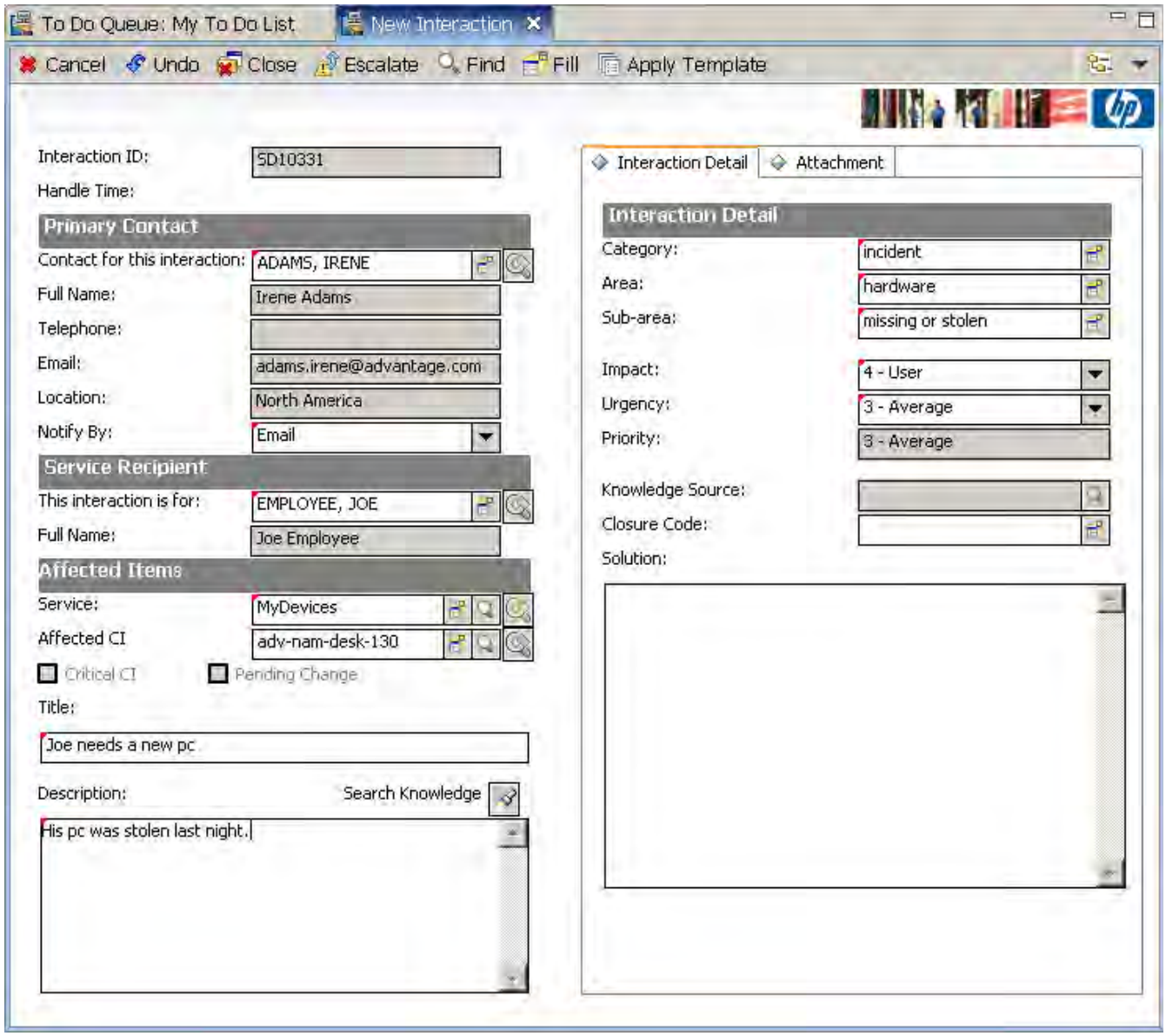

Figure 4-1 A new interaction that has been filled in

Interaction form after escalation

After the Service Desk Agent escalates the interaction, Service Desk displays new fields and tabs.

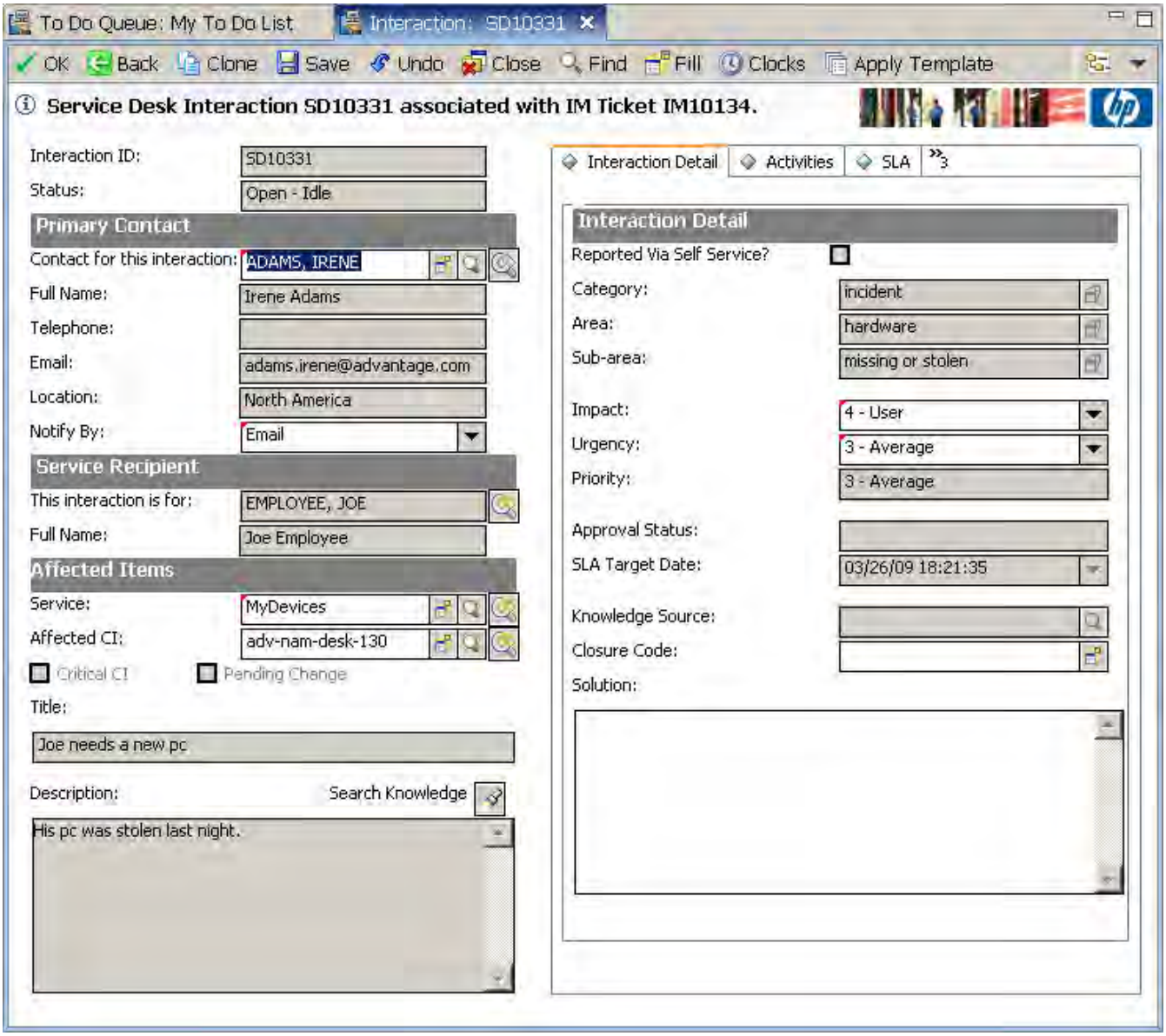

Figure 4-2 The same interaction after escalation

User Interaction Management form details

The following table identifies and describes some of the features on Service Desk's User Interaction Management forms.

Table 4-1 User Interaction Management form details

Label	Description
Interaction ID	Service Manager populates this field with a unique ID when a Service Desk Agent registers a new interaction.
Primary Contact Contact for this interaction	The Service Desk Agent populates this field with the contact name related to the company from which this call was received for this interaction. The contact person is not necessarily the same person as the service recipient. This field ensures that the correct person will be notified about updates to the interaction. Filling in this field auto-populates the Full Name, Telephone, Email, and Location fields with information from the contact record. After filling in the contact name, the Service Desk Agent can use the Smart Indicator positioned at the end of the field to view open or closed interactions for this contact. This is a required field.
Primary Contact Notify By	To notify the customer when the issue has been resolved, Service Manager prepopulates this field with Email. The Service Desk Agent can change it to None or Telephone, if applicable. When the related incident or change is closed: • Selecting Email sends email to the contact and closes the interaction • Selecting None closes the interaction without notifying the contact • Selecting Telephone sets the interaction to the status Open-Callback, which tells the Service Desk Agent to call the contact. The Service Desk Agent asks the contact whether the solution is satisfactory and indicates the answer on the Required Actions tab. If the solution works for the customer, you close the interaction. If it does not work, then you must reopen the incident. This is a required field.
Service Recipient This interaction is for	The person who has the problem and needs it resolved. It is not necessarily the person who is calling to report the problem. Filling in this field automatically fills in the contact name from the contact record of who should be notified of the resolution. The Service Desk Agent populates this field with the person this issue is registered for. When the primary contact is also the service recipient, Service Manager fills this field in after the service is selected. After filling in the service recipient, the Service Desk Agent can use the Smart Indicator positioned at the end of the field to view open or closed interactions for this contact. This is a required field.

Table 4-1 User Interaction Management form details

Label	Description
Affected Items Service	The Service Desk Agent populates this field with the business service affected by the registered issue. Only business services the service recipient has a subscription for can be selected. As a best practice, users should select the affected service before selecting the Affected CI because the Affected CI selection is limited by the service selected by a user. Selecting the service first prevents a mismatch between the service and the CI. ITIL V3 is centered around services, so a service construct should always be defined for best practices. If you have not yet created a service construct, start with a catch-all service, such as My Devices. Note: The out-of-box options in this field are based on past Service Manager implementations. You should tailor these options to match your business needs. These business services are available out-of-box: • Applications • E-mail/Webmail • Handheld PDA & Telephony • Intranet • Internet • My Devices (The My Devices service represents all personal devices that the user would use.) • Printing Selecting the service: • May limit the list of affected CIs. • Validates that it is a valid service An end user is more likely to know that the e-mail service does not work than what part of the e-mail service does not work. This is a required field. Tip: You can use the Smart Indicator, positioned at the end of the field, to search for related incidents or problems.
Affected Items Affected CI	The Service Desk Agent populates this field with the configuration item (CI). Click Fill to select from a list of the physical CIs that relate to the service. Other CIs can be entered manually. If the business service does not contain any CIs, then the list shows only the CIs that the service recipient is subscribed to and the CIs that are assigned to the service recipient. If you choose an application, you are presented with a list of CIs in the service, as well as those that you own. After filling in the affected CI, the Service Desk Agent can use the Smart Indicator positioned at the end of the field to search for open and closed incidents for this CI, and to view the details.
Title	The Service Desk Agent populates this field with a brief description that identifies the interaction. Note: Service Manager searches this field when you do an advance or expert text search. This is a required field.

Table 4-1 User Interaction Management form details

Label	Description
Description	The Service Desk Agent populates this field with a detailed description of the interaction. When the location and telephone number differ from the contact details, the Service Desk Agent can record the correct information in the description field. Clicking Search Knowledge searches description fields across multiple Service Manager knowledgebases for the text entered. Depending on the permissions of the user, Service Manager may look in interactions, incidents, problems, known errors, and knowledge documents. The Service Desk Agent can use the solution from any returned document as the solution for the interaction. Note: Service Manager searches this field when you do an advance or expert text search. This is a required field.
Interaction Detail	The Interaction Detail notebook is based on a classification structure, such as a cost code and closure analysis, to classify interaction records for reporting purposes. This is a required field.
Interaction Detail > Category	This field describes the type of interaction. The interaction type determines the process to escalate to when the interaction cannot be solved on first intake. The categories are based on ITIL service-centric processes, and therefore focus on enabling ticket assignment, reporting, and operational analysis for knowledge management purposes. From the category dropdown: • Complaint > Escalate — Service Manager creates a new incident. • Incident > Escalate — You can relate the interaction to an existing incident, an existing known error, or create a new incident. • Request for Change > Escalate — Service Manager creates a new change request. • Request for Information > Escalate — Service Manager creates a new incident. • Options menu > Order from Catalog — Service Catalog opens, allowing you to place an order. The interaction is given the category service catalog. Service Catalog interactions are not escalated. When you approve the interaction, it opens the related record as defined in the service catalog connector. For more information on Categories and the areas and subareas associated with them, see Interaction categories on page 50. This is a required field.
Interaction Detail > Area	The Service Desk Agent populates this field with the area of concern. Service Manager displays different lists of areas, depending on the category you selected. For more information on categories and the areas and subareas associated with them, see Interaction categories on page 50. This is a required field.
Interaction Detail > Sub-area	The third level of classifying an interaction, mainly used for reporting purposes. Service Manager displays different lists of sub-areas, depending on the area you selected. For more information on categories and the areas and sub-areas associated with them, see Interaction categories on page 50. This is a required field.

Table 4-1 User Interaction Management form details

Label	Description
Interaction Detail > Impact	The Service Desk Agent populates this field with the impact the interaction has on the business. The impact and the urgency are used to calculate the priority. The impact is based on how much of the business is affected by the issue. The stored value can be 1-4, as follows. • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User This is a required field.
Interaction Detail > Urgency	The urgency indicates how pressing the issue is for the service recipient. The urgency and the impact are used to calculate the priority. The stored value can be 1-4, as follows. • 1 - Critical • 2 - High • 3 - Average • 4 - Low This is a required field.
Interaction Detail > Priority	This field describes the order in which to address this interaction in comparison to others. It contains a priority value calculated by (impact + urgency)/2. Decimals are truncated. The stored value based on that calculation can be 1-4, as follows: • 1 - Critical • 2 - High • 3 - Average • 4 - Low
Interaction Detail > Knowledge Source	This field contains the reference number of the document from the knowledgebase document used to solve the issue. If you find a knowledge article by using Search Knowledge, and then click Use Knowledge in that article to provide the solution to your customer, this field is populated with the Document ID of the document you used. If you do not use a knowledge document or if you do not click Use Knowledge in the knowledge document, this field is left blank.

Table 4-1 User Interaction Management form details

Label	Description
Interaction Detail > Closure Code	This field contains a predefined closure code, describing the way this issue has been solved. The out-of-box options in this field are based on Service Manager customer reference data. Tip: You may want to tailor these options to match your business needs. These closure codes are available out-of-box: • Not Reproducible • Out of Scope • Request Rejected • Solved by Change/Service Request • Solved by User Instruction • Solved by Workaround • Unable to solve • Withdrawn by User
Interaction Detail > Solution	This field contains a description of the solution used for this interaction. Note: Service Manager searches this field when you do an advance or expert text search.
Status	Service Manager populates this field with a predetermined status when a Service Desk Agent closes or escalates and interaction. The options in this field have been revised to align with our new best practices. Tip: You may want to tailor these options to match your business needs. These statuses are available out-of-box: • Open-Idle — The interaction has no incidents, changes, or other records related to it. The call has been opened, but not escalated or closed. For example, when the Service Desk Agent is still on the phone with the customer, or when a self-service user has created a request. • Open-Linked — The call has been escalated or the catalog request approved and the interaction is now related to another record, such as an incident, change, or request. • Open-Callback — There is an action pending for the interaction. The Service Desk Agent must now call the contact. When the related record is closed, the interaction is automatically set to open-callback. if the Notify By field is set to telephone for that user. • Closed — The interaction was closed by the help desk or automatically after the related record was closed.
Approval Status	This field is only used when you request something from the catalog. When you submit an order from the catalog, Service Manager automatically creates an interaction which, based on approval requirements, may have to be approved before it can be fulfilled. Service Manager populates this field with the current approval status for this interaction. These approval statuses are available out-of-box: • Pending — The request has not been approved or a prior approval or denial has been retracted. • Approved — All approval requirements are approved, or no approval necessary • Denied — The request has been denied.

Table 4-1 User Interaction Management form details

Label	Description
Activities	The Activities notebook records information that the Service Desk Agent enters during the lifecycle of the ticket. Every time you update an interaction, you must fill in an update on the Activities notebook (Update sub-notebook). A log of all the updates is stored on the Journal Updates and Historic Activities tabs. Activities from related records that are flagged as customer visible are also displayed here.
Related Records	The Related Records notebook contains a list of all related records for the interaction. These may include related incidents, known errors, changes, and quotes.
SLA	The SLA (Service Level Agreement) notebook displays SLAs related to the interaction. SLAs in interactions are customer-related and selected, based on the customer contact or department and service related to the issue. The Service Level Objective (SLO) defines the details, such as beginning and ending state, and time allowed between these states. SLA selection takes place when a Service Desk Agent escalates the interaction. The best practice is that the Service Desk Agent should communicate the time of the next breach to the customer at this point. If SLAs are configured to be handled in the background, the information on this tab may not display immediately. Note: The out-of-box system is set up to run SLAs in the foreground. Tailoring the system to run SLAs in the background complicates communicating with the customer and should be avoided.
Escalate button	The Service Desk Agent clicks this button to create an incident from this interaction. The customer's issue could not be solved immediately. When research time is required, the ticket should be escalated to an incident or a change, not saved as an interaction. There is no monitoring on saved interactions, other than self-service interactions. If the Service Desk has a role in the Incident Management process, this incident may be assigned to the Service Desk, and the Service Desk Agent can still work on it. Clicking Escalate starts the Escalate Interaction wizard. Tip: You may want to tailor the Escalate Interaction - Incident wizard to prepopulate desired information. For more information on the Escalate Interaction wizard, see Escalate Interaction wizard on page 52
Undo button	The Service Desk Agent clicks this button to reload the last saved version of a submitted self-service ticket, or to clear all data from the screen. Note: All changes after the last save will be lost.
Close button	The Service Desk Agent clicks this button to close the interaction. The customer's issue was resolved and requires no further action.

Interaction categories

The category hierarchy was designed to support the ITIL V3 model of service-centric support. It is a natural-language-based hierarchy meant to enable the Service Desk Agent to easily classify the ticket. The three-level hierarchy (category, area, and sub-area) creates a “sentence” that clearly and uniquely defines the issue without ambiguity.

The category determines which process the record belongs to. Combined with the area and subarea, it also is used for to report results and to determine the knowledgebase assignment for the event.

Since the category values represent best practices, customizing this data is not expected. The area and subarea fields can be customized; however, they should cover the scope of the IT Service provisioning in natural language definition and should remain unmodified. If you choose to customize the areas and subareas, be sure to set them up in a natural easy-to-follow hierarchy.

The categories, areas, and subareas that come with Service Desk out-of-box are captured in this table.

Table 4-2 Categories, areas, and subareas

Category	Area	Sub-area
complaint	service delivery	availability
complaint	service delivery	functionality
complaint	service delivery	performance
complaint	support	incident resolution quality
complaint	support	incident resolution time
complaint	support	person
incident	access	authorization error
incident	access	login failure
incident	data	data or file corrupted
incident	data	data or file incorrect
incident	data	data or file missing
incident	data	storage limit exceeded
incident	failure	error message
incident	failure	function or feature not working
incident	failure	job failed
incident	failure	system down
incident	hardware	hardware failure
incident	hardware	missing or stolen
incident	performance	performance degradation
incident	performance	system or application hangs
incident	security	security breach

Table 4-2 Categories, areas, and subareas (cont'd)

Category	Area	Sub-area
incident	security	security event/message
incident	security	virus alert
problem	access	authorization error
problem	access	login failure
problem	data	data or file corrupted
problem	data	data or file incorrect
problem	data	data or file missing
problem	data	storage limit exceeded
problem	failure	error message
problem	failure	function or feature not working
problem	failure	job failed
problem	failure	system down
problem	hardware	hardware failure
problem	hardware	missing or stolen
problem	performance	performance degradation
problem	performance	system or application hangs
problem	security	security breach
problem	security	security event/message
problem	security	virus alert
request for change	service portfolio	new service
request for change	service portfolio	upgrade / new release
request for information	general information	general information
request for information	how to	how to
request for information	status	status
service catalog	service catalog	service catalog

Escalate Interaction wizard

Depending on your selection, the Escalate Interaction wizard opens one of the following wizards:

- Escalate Interaction - Complaint wizard

  The Escalate Interaction - Complaint wizard creates a new incident ticket in the background, and assigns it to the Service Desk Manager.

- Escalate Interaction - Incident wizard

  The Escalate Interaction - Incident wizard requests further information, including location and assignment, and creates an incident ticket.

  Each CI has a location.code that it is assigned to, and each device has an assignment group it defaults to. If the CI is at a different location from its default, the location information is important to the person assigned to the incident. The system generates a list of all assignment groups for the selected service or CI. The Service Desk Analyst can only assign the interaction to a listed service or CI.

  The location information is used for dispersed global assignment groups. The information can be used in inboxes to show only incidents local or close to the technician's location.

  When you relate the incident to a known error (KE), you can call the Escalate Interaction - Incident-KE wizard. If the Service Desk Analyst selects a KE, the system presents the workaround from that KE to the Service Desk Analyst to validate and to add interaction-specific information. The workaround text is subsequently used as the solution text for the interaction.

- Escalate Interaction - RFI wizard

  The Escalate Interaction - RFI wizard creates a new incident ticket in the background with the default category Request for Information (RFI). The RFI incident ticket is assigned to the Service Desk assignment group.

- Escalate Interaction - RFC wizard

  The Escalate Interaction - RFC wizard creates a new change request in the background, in the review phase, with the category "default".

5 Incident Management Overview

The HP Service Manager Incident Management application, referred to as Incident Management throughout this chapter, supports the Incident Management process. It provides comprehensive Incident Management that allows you to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

Incident Management enables you to categorize and track various types of incidents (such as service unavailability or performance issues and hardware or software failures) and to ensure that incidents are resolved within agreed on service level targets.

This section describes how Incident Management implements the best practice guidelines for the Incident Management processes.

Topics in this section include:

Incident Management within the ITIL framework

Incident Management is addressed in ITIL's *Service Operation* publication. The document describes Incident Management as the process responsible for restoring normal service operation as quickly as possible.

The ITIL publication points out that Incident Management is highly visible to the business, and therefore it is often easier to demonstrate its value in comparison to other areas of Service Operation. These values include:

- the ability to detect and resolve incidents, resulting in lower downtime and higher service availability
- the ability to align IT activity to real-time business priorities
- the ability to identify potential improvements to services, and additional service or training requirements

Incident Management application

The Incident Management application automates reporting and tracking of a single incident or a group of incidents associated with a business enterprise. It enables you to categorize types of incidents, and keep track of their resolution.

With Incident Management, the appropriate people can escalate and reassign incidents. Incident Management can also automatically issue alerts or escalate an incident to properly meet the agreed-upon terms of the service contract. For example, if a network printer is disabled, a technician or manager can escalate the incident to a higher priority to ensure that the incident is fixed quickly.

Incident Management restores normal service operation as quickly as possible and minimizes the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. It includes events that are communicated directly by Users, either through the Service Desk or through an automated interface between Event Management and Incident Management tools.

Incident Management defines normal service operation as service performance to meet Service Level Agreement (SLA), Operation Level Agreement (OLA), and Underpinning Contract (UC) targets.

Incidents can be reported and logged by support staff, who may notify the Service Desk if they notice an issue. Not all events are logged as incidents. Many classes of events are not related to disruptions at all, but are indicators of normal operation or are simply informational.

Notes for Incident Management implementation

The new Incident Management best practices make some changes you may want to take into consideration when implementing your updated system.

Incident Closure process

Service Manager includes the Service Desk application to perform user interaction activities. Service Manager is configured out-of-box to use a one-step Incident Closure process. Therefore, incident personnel can close the incident directly after resolving it. The Service Desk takes care of notifying the end user and closing the interaction that initiated the incident.

Legacy Service Manager customers who did not activate Service Desk and used a two-step incident close will find that this is no longer necessary, because the Service Desk application is now included.

Incident ticket information

The incident ticket includes the information essential to assigning and addressing the incident. It does not include contact information for the person who initiated the incident, for several reasons. First, several contacts could be directly related to a single incident. If only the contact information for the first was recorded, the analyst might only focus on that customer and not check for related interactions. In addition, contact and customer related data is stored in the interaction record, as the Interaction Management process defines the transition point between the end user and IT.

Although the incident ticket does not directly display the information about the person who initiated the incident, that information can be easily retrieved by using the Options menu to view any interaction records that are related to the incident.

Incident Management process overview

The Incident Management process includes all necessary steps to log and resolve an incident, including any necessary escalations or reassignments. Monitoring of Service Level Agreements (SLAs), Operation Level Agreements (OLAs), and Underpinning Contracts (UCs) are also part of the overall process.

When an incident ticket is opened, the associated SLA starts tracking the time that elapses. The Incident Coordinator assigns the ticket to an Incident Analyst for investigation and diagnosis. If necessary, the ticket can be reassigned to a different assignment group.

A general overview of the Incident Management processes and workflows is depicted in Figure 5-1,below. They are described in detail in Chapter 6, Incident Management Workflows.

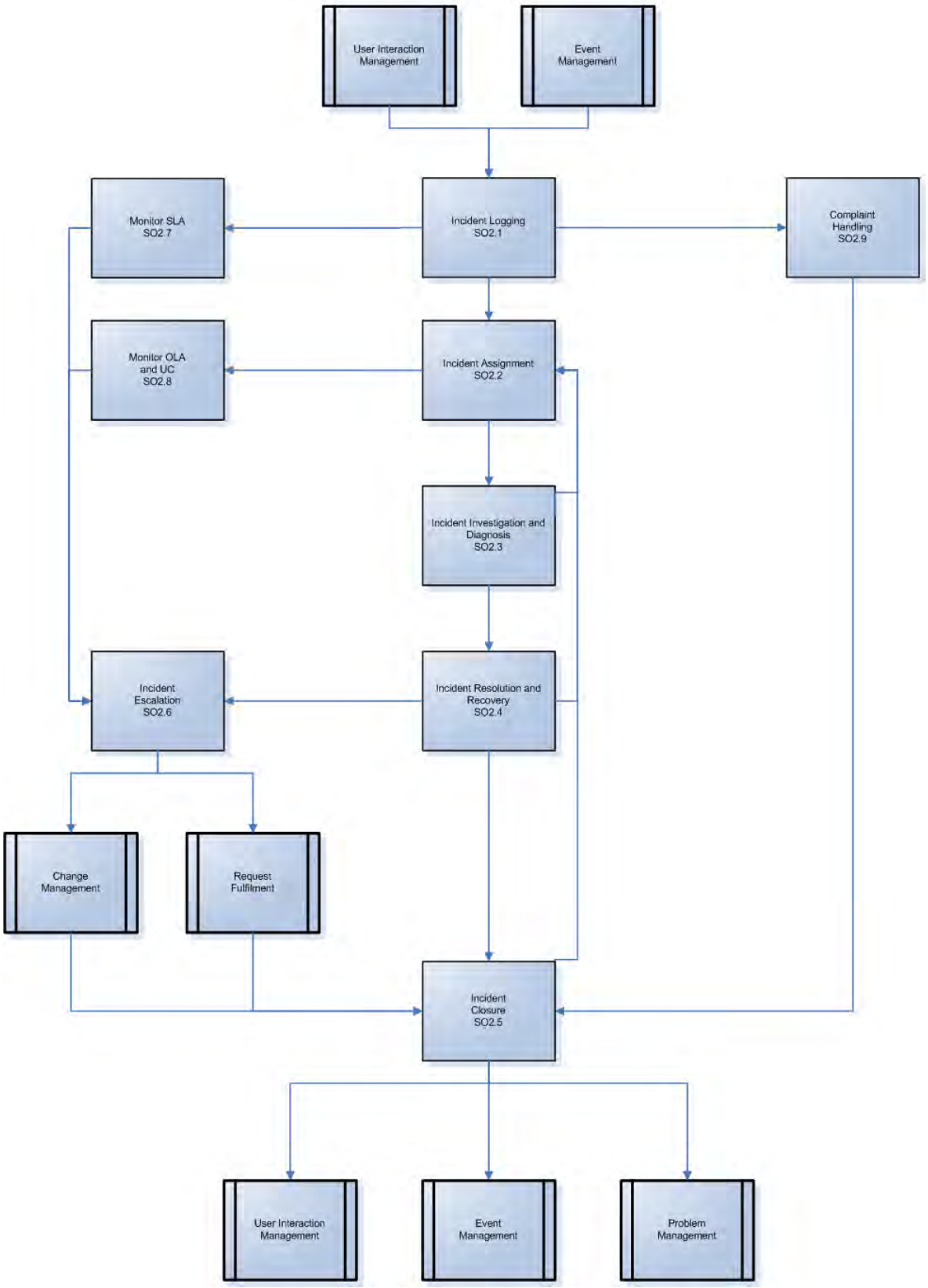

Figure 5-1 Incident Management process diagram

Incident Management user roles

Table 5-1 describes the responsibilities of the Incident Management user roles.

Table 5-1 Incident Management User Roles and Responsibilities

Role	Responsibilities
Operator	Registers incidents based on an event and assigns them to the correct support group.
Incident Analyst	• Reviews and accepts or rejects assigned incidents. • Investigates and diagnoses incidents. • Documents incident resolutions or workarounds in the Service Management application. • Implements incident resolutions. • Verifies that incidents are resolved and closes them.
Incident Coordinator	• Reviews and accepts or rejects incidents assigned to the support group. • Handles incidents escalated by an Incident Analyst of the support group. • Monitors Operational Level Agreements (OLA) and Underpinning Contracts (UC) targets of the support group.
Incident Manager	• Handles incidents escalated by the Incident Coordinator or by the Service Desk Agent. • Determines and executes the appropriate escalation actions. • Requests an Emergency Change, if required.
Service Desk Manager	Handles incidents that are categorized as Complaints.

Input and output for Incident Management

Incidents can be triggered and resolved in several ways. Table 5-2 outlines the inputs and outputs for the Incident Management process.

Table 5-2 Input and output for Incident Management

Input to Incident Management	Output from Incident Management
• Customer interactions with the Service Desk, which can be escalated to incidents • Event management tool, which automatically opens incidents • Support staff. *	• Resolved incidents • Documented workarounds, solutions, or knowledge articles • New problems, changes, or incidents Incidents can also trigger several other Service Manager processes, as described in the next section.

* Service Manager user roles assigned to staff who can open incidents directly include Incident Managers, Incident Coordinators, Configuration Auditors, Operators, Request Administrators, Request Procurement Managers, and System Administrators.

Key performance indicators for Incident Management

The Key Performance Indicators (KPIs) in Table 5-3 are useful for evaluating your Incident Management processes. To visualize trend information, it is useful to graph KPI data periodically. In addition to the data provided by Service Manager, you may need additional tools to report on all of your KPI requirements.

Table 5-3 Key Performance Indicators for Incident Management

Title	Description
% of incidents closed within SLA target time	The number of incidents closed within the SLA target time, relative to the number of all incidents closed, in a given time period.
% of reopened incidents	The number of incidents closed that were reopened because the solution was not accepted by the customer, relative to the number of all incidents closed, in a given time period.
Backlog of incidents	The number of incidents that are not yet closed, in a given time period.
Total number of incidents	Total number of new reported incidents, in a given time period.

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included below.

ITIL V3 Key Performance Indicators

The following are ITIL V3 KPIs for Incident Management:

- Total number of incidents (as a control measure)
- Breakdown of incidents at each stage (for example, logged, work in progress, and closed)
- Size of current incident backlog
- Number and percentage of major incidents
- Mean elapsed time to achieve incident resolution or circumvention, separated by impact code
- Percentage of incidents handled within target response time; incident response-time targets may be specified in SLAs, for example, by impact and urgency codes
- Average cost per incident
- Number of incidents reopened and as a percentage of the total
- Number and percentage of incidents incorrectly assigned
- Number and percentage of incidents incorrectly categorized
- Number and percentage of incidents resolved remotely, without the need for a visit
- Number of incidents handled by each incident model
- Breakdown of incidents by time of day, which helps pinpoint peaks and ensure matching of resources

COBIT 4.1 Key Performance Indicators

The following are the COBIT 4.1 KPIs for Incident Management:

- Percent of incidents resolved within the time period specified
- Percent of incidents reopened
- Average duration of incidents by severity
- Percent of incidents that require local support (that is, field support or a personal visit)

RACI matrix for Incident Management

A Responsible, Accountable, Consulted, and Informed (RACI) diagram or RACI matrix is used to describe the roles and responsibilities of various teams or people in delivering a project or operating a process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. The RACI matrix for Incident Management is shown in Table 5-4.

Table 5-4 RACI Matrix for Incident Management

Process ID	Activity	Incident Manager	Incident Coordinator	Incident Analyst	Incident Operator	Service Desk Agent	Service Desk Manager	User
SO 2.1	Incident Logging	A	I		R	R		
SO 2.2	Incident Assignment	A	R	R				
SO 2.3	Incident Investigation and Diagnosis	A	C/I	R				C/I
SO 2.4	Incident Resolution and Recovery	A	C/I	R				C/I
SO 2.5	Incident Closure	A	C/I	R	I	I		I
SO 2.6	Incident Escalation	R/A	R	I				
SO 2.7	SLA Monitoring	A/I	I	I		R		
SO 2.8	OLA and UC Monitoring	A/I	R	I				
SO 2.9	Complaint Handling	A/I					R	C/I

6 Incident Management Workflows

The Incident Management process logs, investigates, diagnoses, and resolves incidents. Incidents can be initiated by the escalation of Service Desk interactions or automatically detected and reported by event monitoring tools. The process includes all necessary steps to log and resolve an incident, including any necessary escalations or reassignments.

The Incident Management process consists of the following processes, which are included in this chapter:

Incident Logging (process SO 2.1)

Incidents are initiated and logged as part of the Interaction Management or the Event Management process, depending on the source and nature of the incident. All relevant information relating to incidents must be logged so that a full historical record is maintained. By maintaining accurate and complete incident tickets, future assigned support group personnel are better able to resolve recorded incidents.

- If the incident is logged by the Service Desk Agent, most incident details are already provided by the interaction record. The Service Desk Agent verifies the Assignment Group to make sure the selected group is the most suitable group to solve the incident. If an incident is categorized as a complaint, the Complaint Handling process is triggered.
- If an incident is logged by an Operator, usually by using a system management tool, the incident must be based on the applicable incident model.

Operators and Service Desk Agents can perform the following Incident Logging tasks:

- Create new incident from monitoring system notification (Operator)
- Create new incident from user interaction (Service Desk Agent)
- Review and update incident information (Service Desk Agent)

You can see the details of this process in the following figure and table.

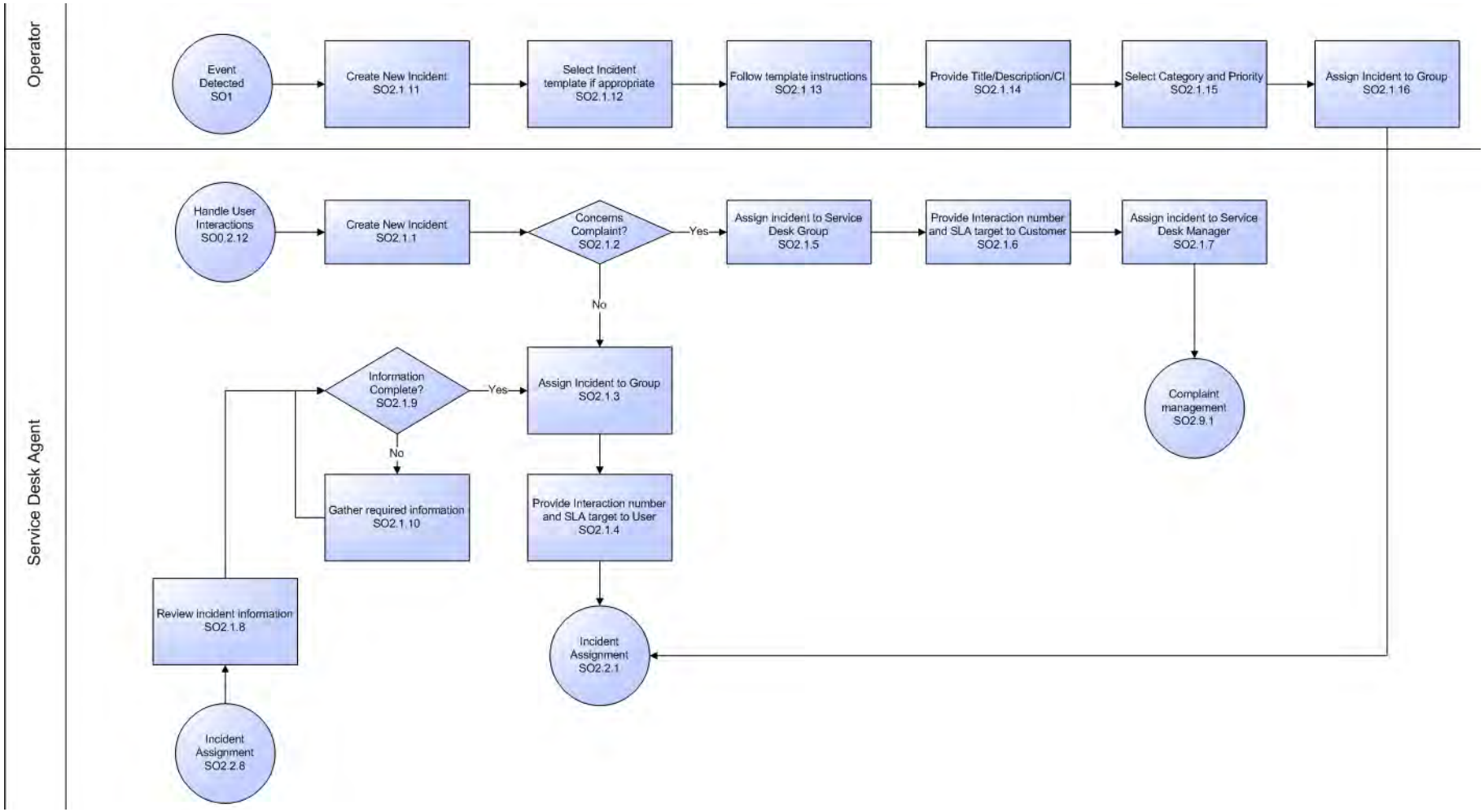

Figure 6-1 Incident Logging workflow

Table 6-1 Incident Logging process

Process ID	Procedure or Decision	Description	Role
SO 2.1.1	Create new incident	A User interaction cannot be solved on first intake and is escalated to the Incident Management process. The interaction is automatically related to the newly created incident. The Service Desk Analyst creates an incident from an interaction.	Service Desk Agent
SO 2.1.2	Categorized as complaint?	Is the incident categorized as a complaint? If yes, go to SO 2.1.5. If no, go to SO 2.1.3	Service Desk Agent
SO 2.1.3	Assign incident to group	Based on the categorization and the affected services, the incident is automatically assigned to the responsible support group. The Service Desk Analyst verifies that the assignment is correct.	Service Desk Agent
SO 2.1.4	Provide interaction number and SLA target to User	The Service Desk Analyst provides the interaction number to the User. The User keeps the interaction number as a reference to the incident. The Service Desk Analyst also provides a target solution date based on the SLA.	Service Desk Agent
SO 2.1.5	Assign complaint incident to Service Desk Group	Incidents categorized as complaints are initially assigned to the Service Desk Group.	Service Desk Agent
SO 2.1.6	Provide interaction number and SLA target to User	The Service Desk Analyst provides the interaction number to the User. The User keeps the interaction number as a reference to the incident. The Service Desk Analyst also provides a target solution date based on the SLA.	Service Desk Agent
SO 2.1.7	Assign incident to Service Desk Manager	After saving, the incident is assigned to the Service Desk Manager (see SO 2.9 Complaint Management).	Service Desk Agent
SO 2.1.8	Review incident information	An incident can be rejected by an assignment group due to incorrect assignment or incomplete information. If this is the case, the Service Desk Analyst reviews the logged comments and corrects the information or assignment.	Service Desk Agent
SO 2.1.9	Information complete?	If no, go to SO 2.1.10. If yes, go to SO 2.1.3. All known errors will have a workaround. The Incident might only remain open for problem tickets. Additionally, the Incident Management process remains responsible.	Service Desk Agent
SO 2.1.10	Gather required information	Gather the missing required information and update the incident with the information. Contact the User if necessary.	Service Desk Agent
SO 2.1.11	Create new incident	An incident is detected when monitoring the Information and Communication Technology (ICT) infrastructure. The Operator (or Initiator) decides to open an incident ticket manually, or an incident ticket is opened automatically, depending on the settings.	Operator
SO 2.1.12	Select incident template if appropriate	The Operator (or Initiator) selects an incident template from a list, or a template is selected automatically, depending on the settings.	Operator
SO 2.1.13	Follow template instructions	The Operator (or Initiator) provides and records the incident details based on the instructions provided by the incident template. The template instructions may filled in by predefined scripts.	Operator

Table 6-1 Incident Logging process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 2.1.14	Provide Title/ Description/CI	Provide a suitable title and description for the incident. This might be based on the event text. If possible, the affected Configuration Item should be selected.	Operator
SO 2.1.15	Select Category and Priority	Select the suitable Category and Priority by selecting the applicable impact level and urgency.	Operator
SO 2.1.16	Assign incident to group	The incident is automatically assigned to the responsible support group, based on the incident categorization and the associated affected services.	Operator

Incident Assignment (process SO 2.2)

Incident tickets are logged from an interaction by a Service Desk Agent or from an event by an Operator. The Incident Coordinator monitors the incident queue, reviews open status incidents, and determines from the information provided whether to accept or reject incident tickets. When an incident ticket is accepted, it is assigned to an Incident Analyst for further investigation and diagnosis.

The Incident Analyst receives an assigned incident and determines whether the incident can be resolved with the tools and knowledge available. If the incident cannot be resolved, the Incident Analyst rejects the incident and reassigns it to the Incident Coordinator.

You can see the details of this process in the following figure and table.

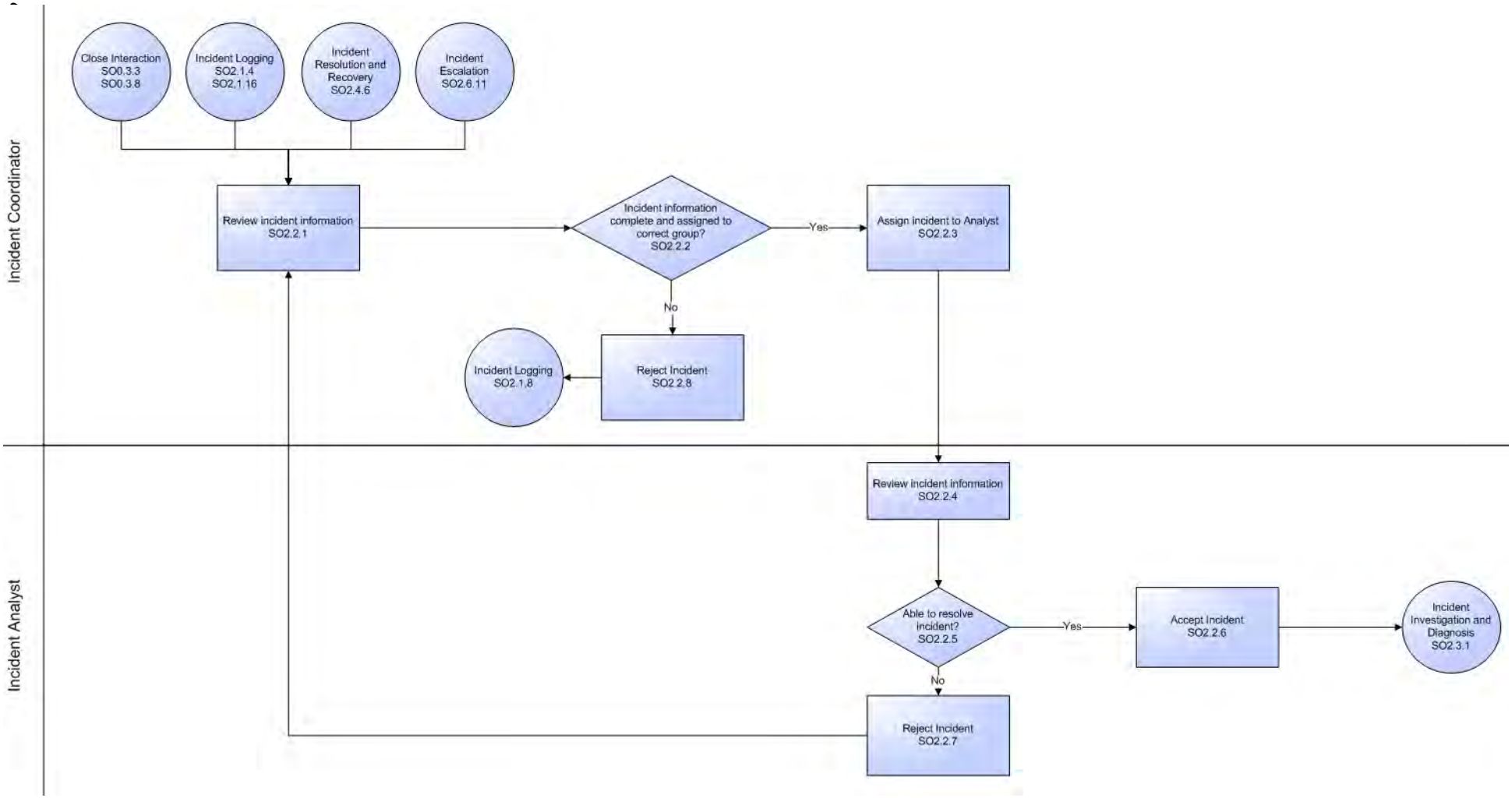

Figure 6-2 Incident Assignment workflow

Table 6-2 Incident Assignment process

Process ID	Procedure or Decision	Description	Role
SO 2.2.1	Review incident information	The Incident Coordinator monitors the incident queue and reviews all incoming Incidents.	Incident Coordinator
SO 2.2.2	Incident information complete and assigned to correct group?	The Incident Coordinator verifies that there is sufficient information available in the incident ticket to diagnose the incident and verifies that the incident is assigned to the correct support group. If yes, continue with SO 2.2.3. If no, go to SO 2.2.8.	Incident Coordinator
SO 2.2.3	Assign incident to analyst	The Incident Coordinator accepts the incident and assigns it to an Incident Analyst from the Incident Coordinator's group for further investigation and diagnosis.	Incident Coordinator
SO 2.2.4	Review incident information	The Incident Analyst monitors the queue of incidents assigned to him/her and reviews the incoming incidents.	Incident Analyst
SO 2.2.5	Able to resolve incident?	The Incident Analyst reviews the assigned incident to see if he/she can resolve it. If yes, continue with SO 2.2.6. If no, go to SO 2.2.7.	Incident Analyst
SO 2.2.6	Accept incident	The Incident Analyst accepts the incident by changing the status to Accepted.	Incident Analyst
SO 2.2.7	Reject incident	The Incident Analyst rejects the incident by clearing the Assignee field, updating the Status field to Rejected, and then providing an update in the Activities tab that states the reason for the rejection. When the Incident Analyst completes the updates, the incident ticket is saved. The incident ticket is then returned to the incident queue for reassignment by the Incident Coordinator.	Incident Analyst
SO 2.2.8	Reject incident	The Incident Coordinator rejects the incident and reassigns it to the Service Desk.	Incident Coordinator

Incident Investigation and Diagnosis (process SO 2.3)

Each support group involved with handling incidents must perform investigation and diagnosis tasks to determine the categorization of and solution to the incident. All actions performed by support group personnel are documented in the incident ticket, so that a complete historical record of all activities is maintained at all times.

Incident Investigation and Diagnosis includes the following actions:

- Establishing the exact cause of the incident
- Documenting user requests for information or for particular actions or outcomes
- Understanding the chronological order of events
- Confirming the full impact of the incident, including the number and range of users affected
- Identifying any events that could have triggered the incident (for example, a recent change or user action)
- Searching known errors or the knowledgebase for a workaround or resolution
- Discovering any previous occurrences, including previously logged incident or problem tickets and known errors, the knowledgebase, and error logs and knowledgebases of associated manufacturers and suppliers
- Identifying and registering a possible resolution for the incident

The Incident Analyst asks the following questions to determine how to resolve an incident:

- Is there a problem, or do I need to provide information for a user's request for information (RFI)?
- Do I have the knowledge and tools to solve this problem?
- Can the incident be reproduced?
- Can the incident be related to an open problem or known error?
- Was the incident caused by the implementation of a change?
- Can a solution be found for this incident?

You can see the details of this process in the following figure and table.

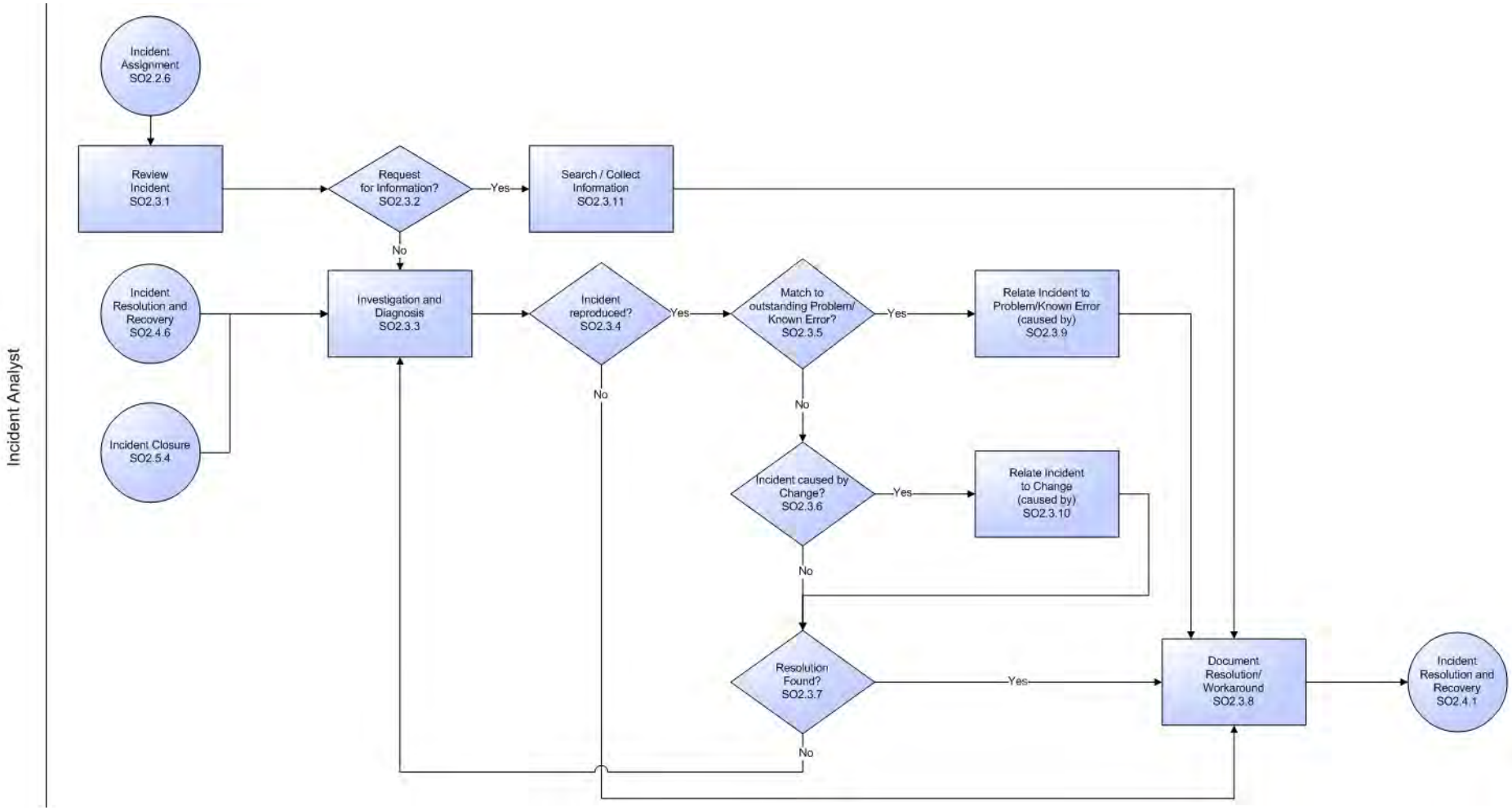

Figure 6-3 Incident Investigation and Diagnosis workflow

Table 6-3 Incident Investigation and Diagnosis process

Process ID	Procedure or Decision	Description	Role
SO 2.3.1	Review incident	The Incident Analyst monitors the queue of incidents assigned to him/her and reviews the incoming incidents.	Incident Analyst
SO 2.3.2	Request for information?	The Incident Analyst evaluates the incident to see if it is categorized as a Request for Information (RFI) or if it is a service disruption. If yes, continue with SO 2.3.11. If no, go to SO 2.3.3.	Incident Analyst
SO 2.3.3	Investigate and Diagnose	The Incident Analyst starts to investigate and diagnose the cause of the incident. The status of the incident is set to Work in Progress.	Incident Analyst
SO 2.3.4	Incident reproduced?	The analyst tries to reproduce the incident. If yes, continue with SO 2.3.5. If no, go to SO 2.3.8.	Incident Analyst
SO 2.3.5	Match to outstanding problem/known error?	The Incident Analyst searches the problem database to see if there is already a problem or known error defined for this incident. If yes, continue with SO 2.3.9. If no, go to SO 2.3.6.	Incident Analyst
SO 2.3.6	Incident caused by change?	The Incident Analyst searches the changes database to see if a recent change may have caused the service disruption. If the configuration item associated with the incident is listed, the Incident Analyst can also look at any changes that have recently been performed against this configuration item. The Incident Analyst can also view the configuration item tree to discover if related configuration items could have caused the incident. If yes, continue with SO 2.3.10. If no, go to SO 2.3.7.	Incident Analyst
SO 2.3.7	Resolution found?	The Incident Analyst checks the known error/knowledgebase for a workaround or resolution to this incident, or tries to find a solution. If yes, continue with SO 2.3.8. If no, go back to SO 2.3.3.	Incident Analyst
SO 2.3.8	Document resolution/ workaround	The Incident Analyst documents the solution or workaround in the incident ticket.	Incident Analyst
SO 2.3.9	Relate incident to problem/known error	When an incident matches an outstanding problem or known error, the incident ticket is related to the problem ticket or known error record.	Incident Analyst
SO 2.3.10	Relate incident to change	When the incident is caused by a previous change, the incident ticket is related to the change request. A solution still needs to be found to solve the incident.	Incident Analyst
SO 2.3.11	Search for/collect information	The Incident Analyst searches for information to provide the requested information to the User.	Incident Analyst

Incident Resolution and Recovery (process SO 2.4)

As part of the Incident Resolution and Recovery process, the Incident Analyst identifies and evaluates potential resolutions before those resolutions are applied and escalates incidents as necessary. The Incident Analyst may escalate an incident to the Incident Coordinator, including those incidents that require a change. If the Incident Analyst does not have the required level of permissions to implement a change, the Incident Analyst reassigns the incident to another group that can implement the resolution. As soon as it becomes clear that the assigned support group is unable to resolve the incident or if the target time period for first-point resolution is exceeded, the incident must be immediately escalated.

The objectives of the Incident Resolution and Recovery process are to ensure that:

- Recorded incidents include a resolution or workaround and information is complete.
- Incidents that require a change are escalated to the Incident Coordinator.
- Incidents for which the Incident Analyst has the required level of permissions are tested and implemented by the Incident Analyst in a production environment.
- Any incidents that the Incident Analyst does not have permissions to implement are reassigned to the applicable group for resolution implementation.
- Any implementation errors that occur during incident resolution correctly trigger resolution reversal and reinvestigation and diagnosis of the incident.
- The Incident Analyst initiates all required escalations.

You can see the details of this process in the following figure and table.

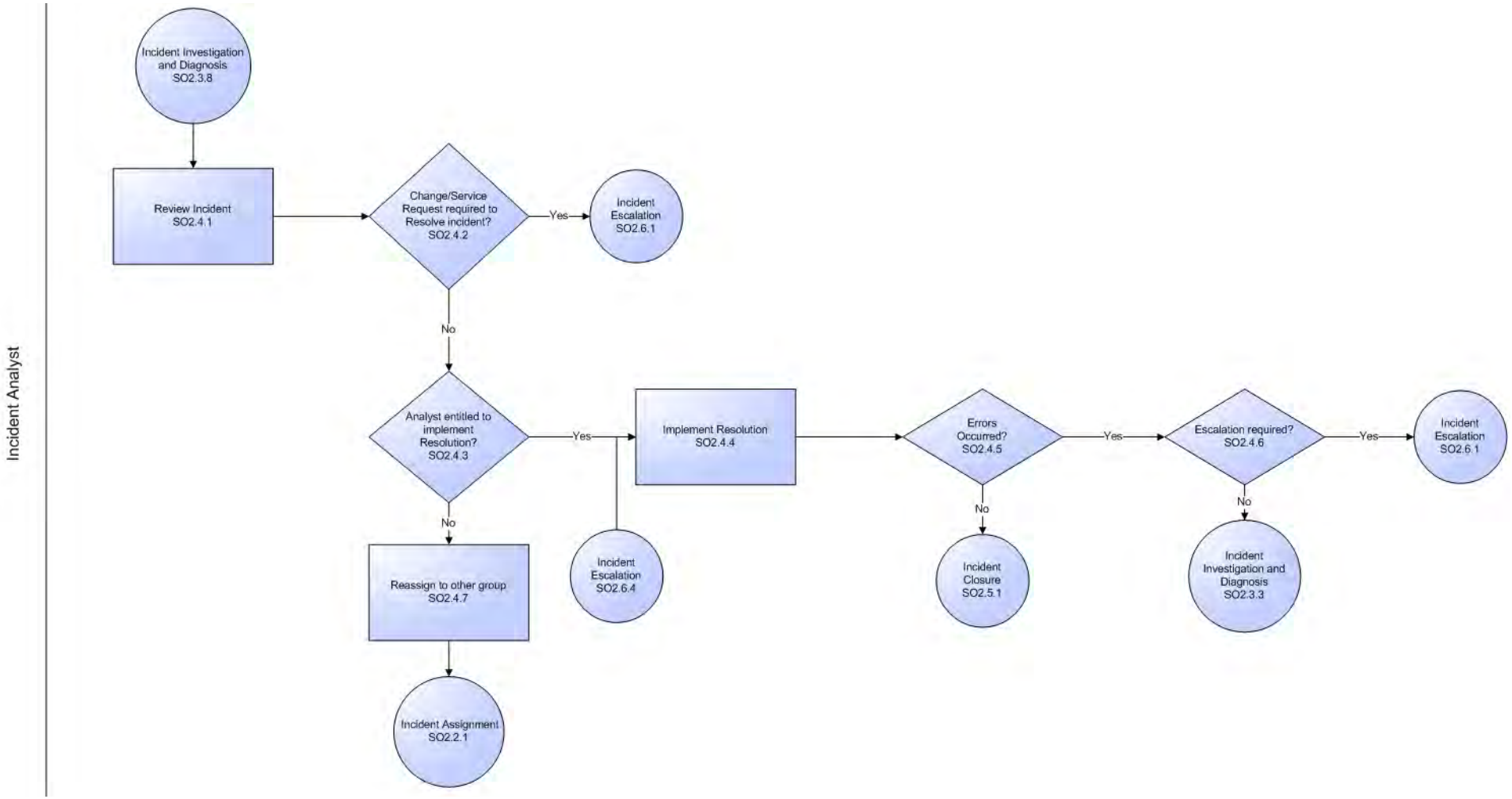

Figure 6-4 Incident Resolution and Recovery workflow

Table 6-4 Incident Resolution and Recovery process

Process ID	Procedure or Decision	Description	Role
SO 2.4.1	Review incident	The Incident Analyst reviews the incident information for the supplied resolution or workaround.	Incident Analyst
SO 2.4.2	Change required to resolve incident?	The Incident Analyst determines whether or not the provided resolution needs to be implemented by using a Change. If yes, go to SO 2.6. If no, continue with SO 2.4.3.	Incident Analyst
SO 2.4.3	Analyst entitled to implement resolution?	The Incident Analyst must judge if he/she has the permissions to implement the resolution. If yes, continue with SO 2.4.4. If no, go to SO 2.4.7.	Incident Analyst
SO 2.4.4	Implement resolution	The Incident Analyst tests the resolution and implements it in the production environment.	Incident Analyst
SO 2.4.5	Errors occurred?	When there are errors during the implementation of a resolution, the Incident Analyst reverses the solution and the incident is returned to the investigation and diagnosis phase. If yes, go to SO 2.4.6. If no, continue with SO 2.5.	Incident Analyst
SO 2.4.6	Escalation required?	Determine if escalation to the Incident Coordinator is required at this point in the resolution process. If yes, go to the Incident Escalation process. If no, go to SO 2.3.3.	Incident Analyst
SO 2.4.7	Reassign to other group	When the Incident Analyst is not entitled to implement the solution, the analyst must reassign the incident to a support group that can implement the solution.	Incident Analyst

Incident Closure (process SO 2.5)

The Incident Closure process includes many steps to verify the success of implemented solutions and to verify that incident tickets are accurate and complete.

After a solution is implemented for an incident, the solution must be verified, typically by the group that implemented the solution. If necessary, the user can be contacted to verify the solution. The resolving group closes the incident and notifies the Service Desk to close the related interaction. When closing an incident, it must be checked to confirm that the initial incident categorization is correct. If the category is incorrect, the record must be updated with the correct closure category. If information is missing from the incident ticket, the missing information must be added so that the incident ticket is complete. The final step in the Incident Closure process is determining the likelihood of the incident recurring and choosing the closure category accordingly. The closure category triggers the Problem Management process when applicable.

You can see the details of this process in the following figure and table.

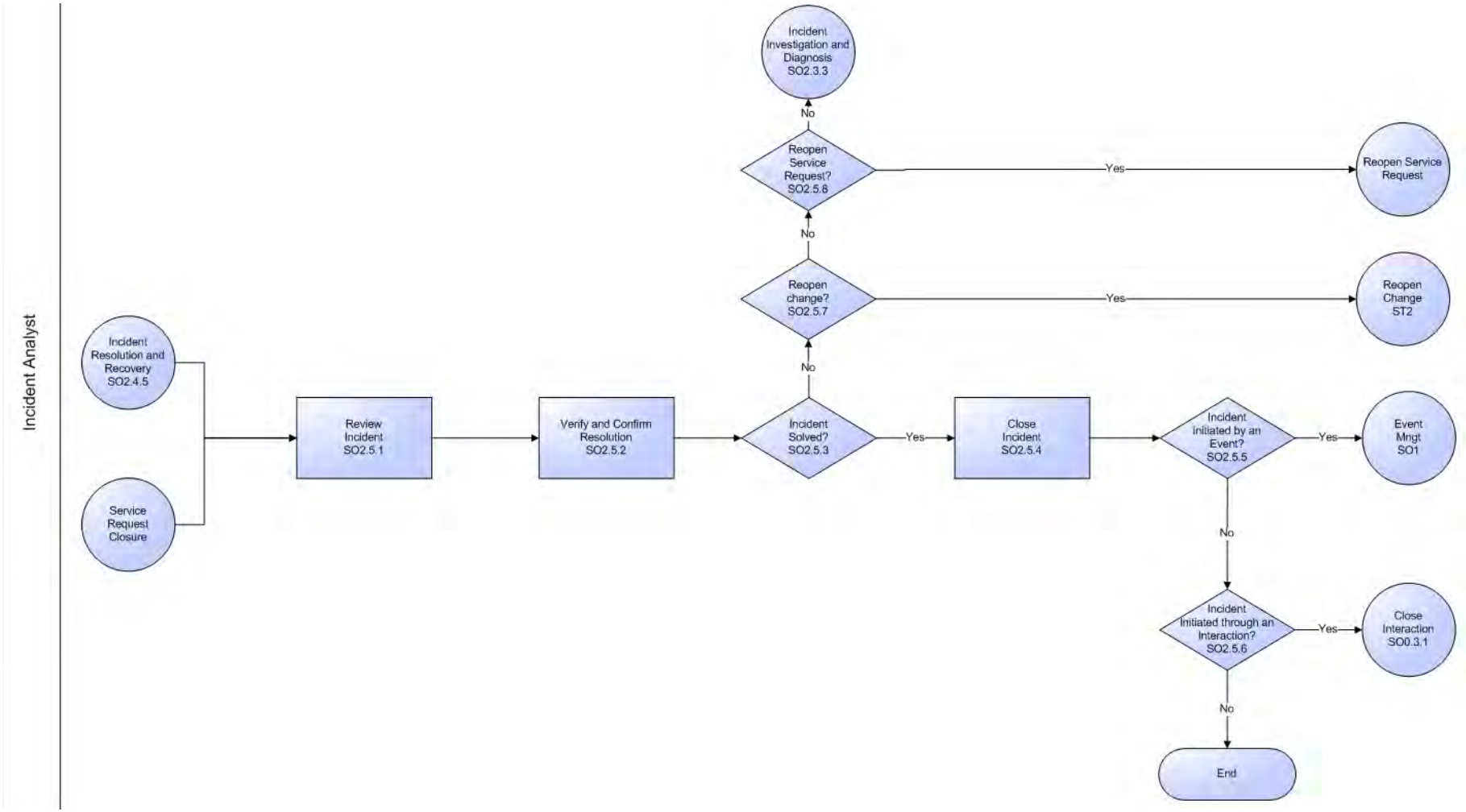

Figure 6-5 Incident Closure workflow

Table 6-5 Incident Closure process

Process ID	Procedure or Decision	Description	Role
SO 2.5.1	Review incident	The Incident Analyst reviews the incident resolution description.	Incident Analyst
SO 2.5.2	Verify and confirm resolution	The Incident Analyst verifies that the resolution is correct and complete and confirms the resolution. If required, the Incident Analyst is entitled to contact the User (see SO 2.7.3) to validate the resolution.	Incident Analyst
SO 2.5.3	Incident solved?	Is the incident solved with the offered resolution? If yes, continue with SO 2.5.4. If no, go to SO 2.5.7.	Incident Analyst
SO 2.5.4	Close incident	The Incident Analyst closes the incident ticket and selects the applicable resolution code.	Incident Analyst
SO 2.5.5	Incident initiated by an event?	Was the incident initiated by an event? If yes, then the event must be confirmed by using the event management process. If no, go to SO 2.5.6.	Incident Analyst
SO 2.5.6	Incident initiated through an interaction?	Was the incident initiated by an interaction? If yes, continue with the Interaction Closure process. If no, then stop.	Incident Analyst
SO 2.5.7	Reopen change?	Was the resolution implemented by using a change that must be reopened? If yes, continue with the reopen change process. If no, go to SO 2.5.8.	Incident Analyst
SO 2.5.8	Reopen service request?	Was the resolution implemented by using a service request that must be reopened? If yes, continue with the reopen change process. If no, go to the incident assignment process.	Incident Analyst

Incident Escalation (process SO 2.6)

When an Incident Analyst is unable to solve an assigned incident within the target time, the analyst escalates the incident to the Incident Coordinator. The Incident Coordinator determines how the incident can best be resolved by consulting the Incident Analyst and, if needed, other Incident Analysts. If an incident is severe (for example, designated as Priority 1), the appropriate IT managers must be notified so that they can anticipate and prepare for an escalation.

Incidents are escalated when the Incident Investigation and Diagnosis process or Incident Resolution and Recovery process exceeds SLA targets or if these targets are likely not to be met. If the steps to resolve an incident are taking too long or proving too difficult, the Incident Coordinator determines the following:

- Whether an Incident Analyst can be given the necessary resources to solve the incident
- Whether a change needs to be implemented
- Whether a request for service is needed

When an incident is escalated, the escalation should continue up the management chain. Senior managers are notified of the situation so that they can prepare to take any necessary actions, such as allocating additional resources or involving suppliers.

You can see the details of this process in the following figure and table.

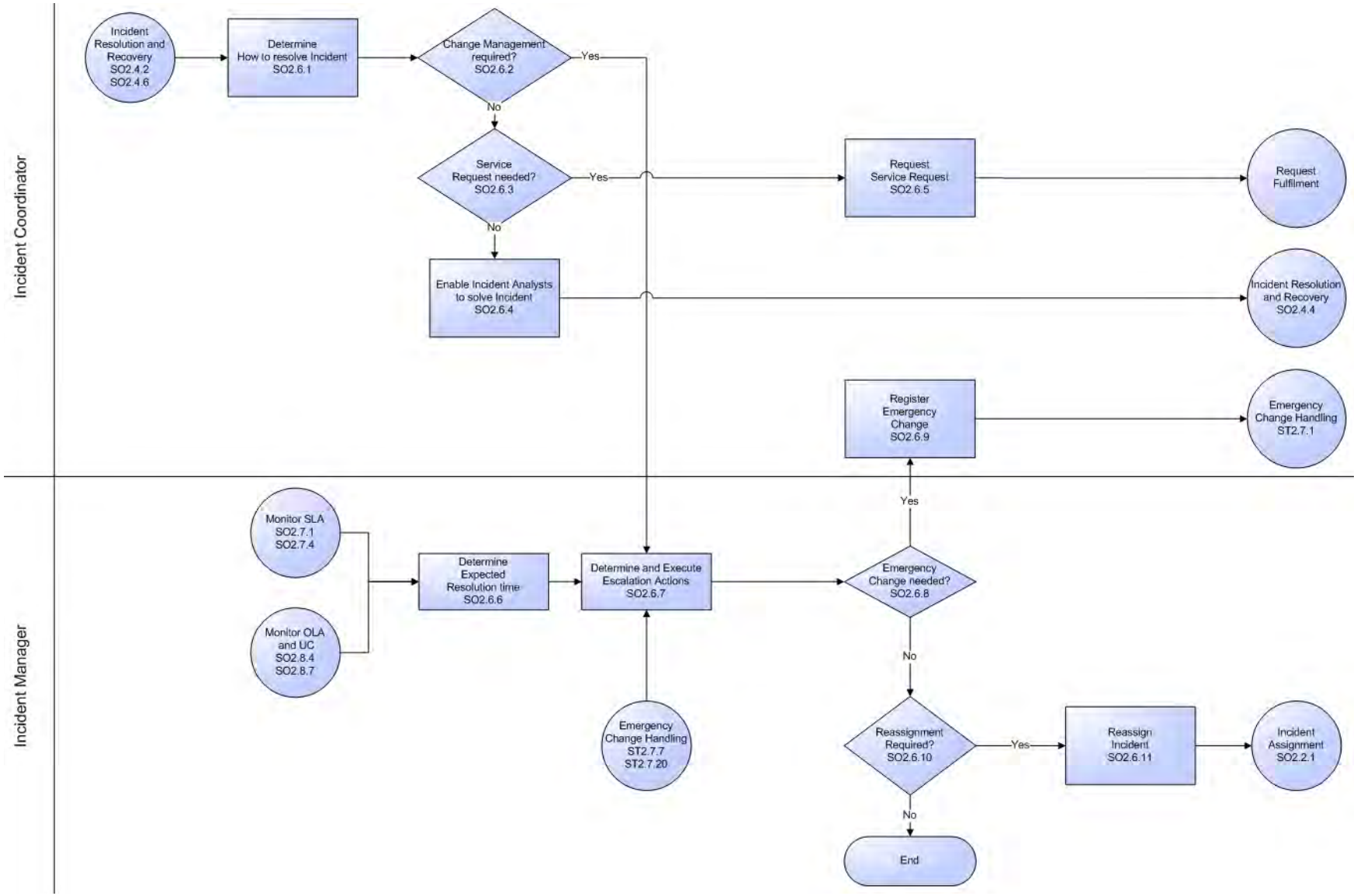

Figure 6-6 Incident Escalation workflow

Table 6-6 Incident Escalation process

Process ID	Procedure or Decision	Description	Role
SO 2.6.1	Determine how to resolve incident	The Incident Coordinator gathers information from the Incident Analyst(s) about the status of the incident resolution and determines how the incident can best be resolved. The Incident Coordinator verifies that the expected resolution time matches any agreed on level, such as that specified in an SLA.	Incident Coordinator
SO 2.6.2	Change Management required?	Is a change required to solve the incident? If yes, continue with SO 2.6.7. If no, go to SO 2.6.3.	Incident Coordinator
SO 2.6.3	Service request needed?	Is it possible to solve the incident with a service request? If yes, continue with SO 2.6.5. If no, go to SO 2.6.4.	Incident Coordinator
SO 2.6.4	Enable Incident Analysts to solve incident	The Incident Coordinator enables the Incident Analyst(s) to focus solely on the resolution of the incident and provides the Incident Analyst(s) with all means necessary to speed up the resolution. Go to SO 2.4.4.	Incident Coordinator
SO 2.6.5	Request service request	The Incident Coordinator completes a service request to implement the proposed resolution by using the request fulfillment process.	Incident Coordinator
SO 2.6.6	Determine expected resolution time	The Incident Manager verifies that the expected resolution time meets SLA targets.	Incident Manager
SO 2.6.7	Determine and execute escalation actions	The Incident Manager determines the actions to be performed to solve the incident within target times and designates escalation personnel to contact in the event of an escalation. This can include determining that the Service Desk is required to send an information bulletin to the affected users and stakeholders.	Incident Manager
SO 2.6.8	Emergency change needed?	If yes, go to SO 2.6.9. If no, go to SO 2.6.10.	Incident Manager
SO 2.6.9	Register emergency change	Based on the Incident Manager's request, the Incident Coordinator registers an emergency change request and contacts the Change Manager to inform the manager about the request, thereby starting the Emergency Change Handling process.	Incident Coordinator
SO 2.6.10	Reassignment required?	Is it necessary to reassign the incident to a different support group with more knowledge (that is, a functional escalation)? If yes, continue with SO 2.6.11. If no, then stop.	Incident Manager
SO 2.6.11	Reassign incident	The Incident Manager reassigns the incident to another 2nd-line or 3rd-line support group.	Incident Manager

SLA Monitoring (process SO 2.7)

Service level agreements (SLAs) contain standards for incident resolution performance. This process describes the activities to monitor all interactions related to incidents from initialization to resolution. SLA Monitoring also determines whether time targets for incident resolution are met, and indicates whether escalation is required to meet the target resolution date according to the associated SLA. SLA Monitoring is an ongoing process performed by the Service Desk.

You can see the details of this process in the following figure and table.

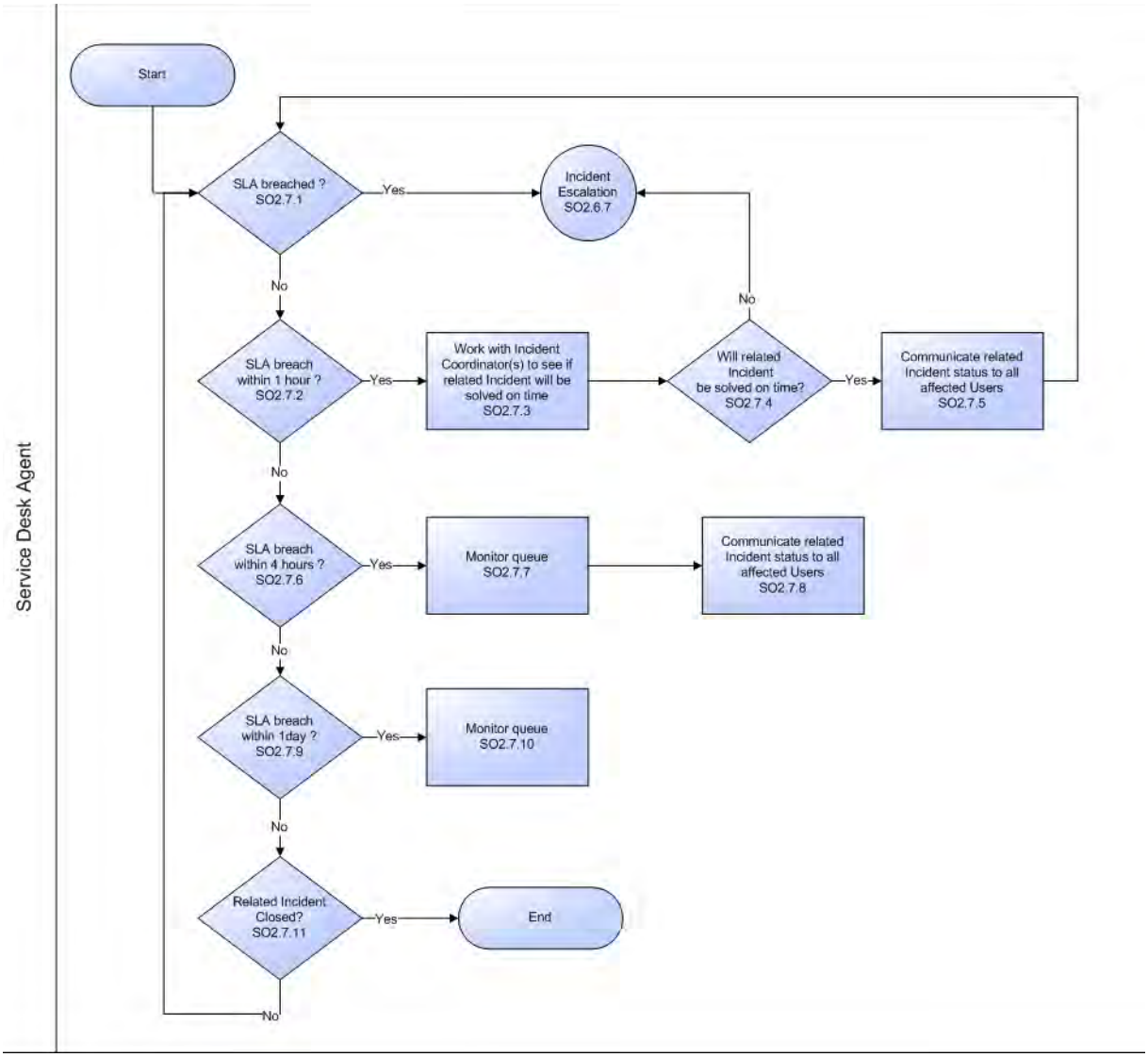

Figure 6-7 SLA Monitoring workflow

Table 6-7 SLA Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 2.7.1	SLA breached?	Has the SLA target date/time been exceeded for this interaction? If yes, start the Incident Escalation process (SO 2.6.7). If no, go to SO 2.7.2.	Service Desk Agent
SO 2.7.2	SLA breach within 1 hour	Does the interaction need to be solved within 1 hour to reach the SLA target date/time? If yes, go to SO 2.7.3. If no, go to SO 2.7.6.	Service Desk Agent
SO 2.7.3	Work with Incident Coordinator(s) to see if incident can still be solved on time	Contact the Incident Coordinator with the related incident assigned to his/her group. Determine whether the group is able to solve the incident on time without further support.	Service Desk Agent
SO 2.7.4	Will related incident be solved on time?	If yes, the Incident Coordinator of the assigned group estimates that the related incident can still be solved on time, go to SO 2.7.5. If no, go to SO 2.6.7 to escalate the incident immediately.	Service Desk Agent
SO 2.7.5	Communicate related incident status to all affected Users	Identify which Users or user groups are affected by the related incident. Send a communication bulletin to inform all affected Users of the incident status and expected resolution time.	Service Desk Agent
SO 2.7.6	SLA breach within 4 hours?	Does the interaction need to be solved within 4 hours to reach the SLA target date/time? If yes, go to SO 2.7.7. If no, go to SO 2.7.9.	Service Desk Agent
SO 2.7.7	Monitor queue	Monitor the interactions within the “Breach within 4 hours queue.”	Service Desk Agent
SO 2.7.8	Communicate related incident status to all affected Users	Identify which Users or user groups are affected by the related incident. Send a communication bulletin to inform all affected Users of the incident status and expected resolution time.	Service Desk Agent
SO 2.7.9	SLA breach within 1 day?	Does the interaction need to be solved within 1 day to reach the SLA target date/time? If yes, go to SO 2.7.10. If no, go to SO 2.7.11.	Service Desk Agent
SO 2.7.10	Monitor queue	Monitor the interaction within the “Breach within 1 day queue.”	Service Desk Agent
SO 2.7.11	Related incident closed?	If yes, no further action is required. If no, go to SO 2.7.1.	Service Desk Agent

OLA and UC Monitoring (process SO 2.8)

One measure of the successful resolution of incidents is the performance of the individual support groups and applicable vendors. The performance of support groups is measured by targets set up within Operation Level Agreements (OLAs). The performance of vendors is measured by targets set up in the Underpinning Contracts (UCs).

The Incident Coordinator monitors all incidents assigned to the support group and applicable vendors. Performance is tracked until incidents are resolved or escalated to meet targeted agreement dates and times. The target date of an OLA and UC usually depends on the priority and category of the incident. The Incident Coordinator can escalate an incident to the Incident Manager if the target time has been or is about to be exceeded.

You can see the details of this process in the following figure and table.

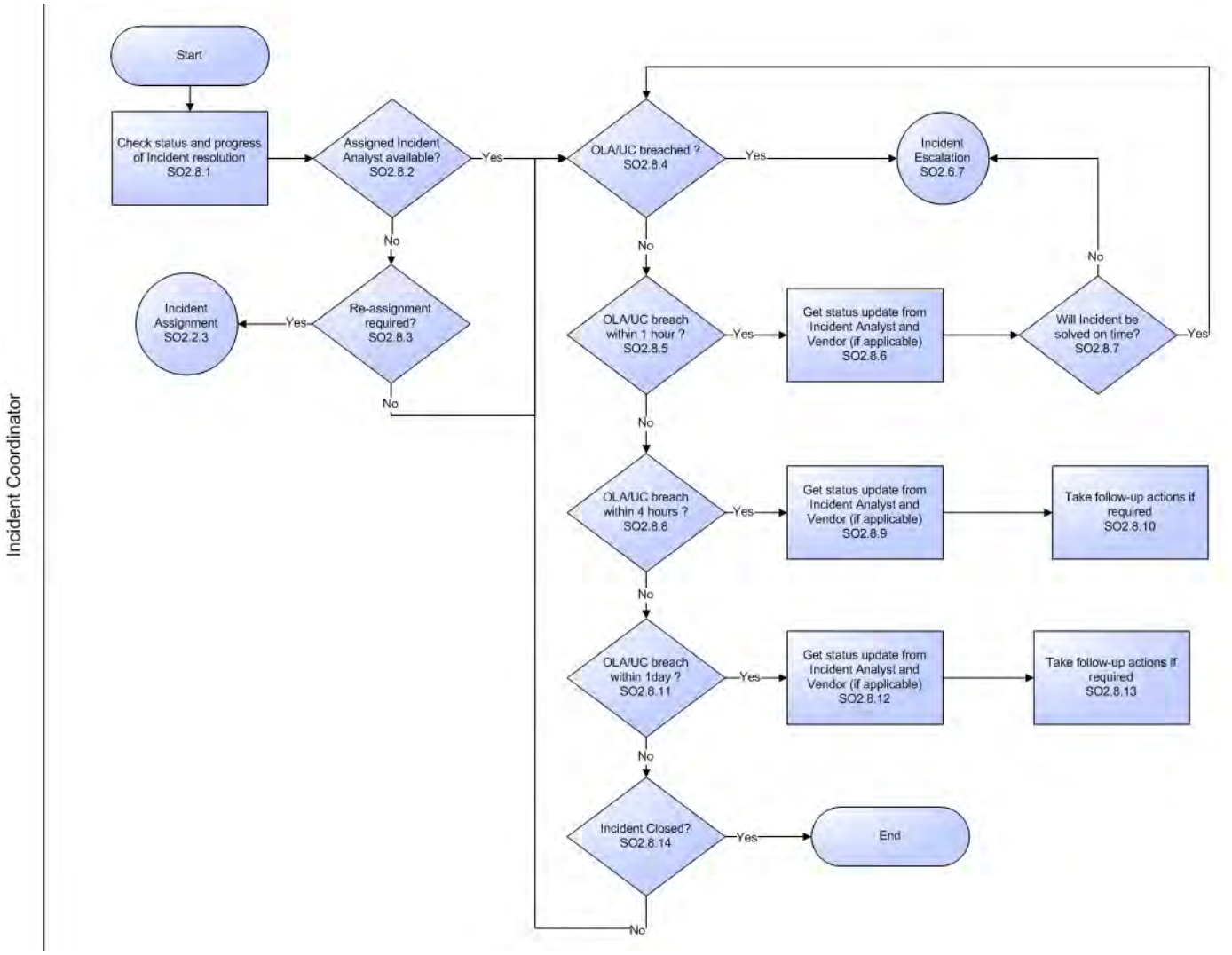

Figure 6-8 OLA and UC Monitoring workflow

Table 6-8 OLA and UC Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 2.8.1	Check status and progress of incident	Check status and progress of incident resolution. Verify that the incident will be resolved before the target date and time specified in applicable Operation Level Agreement (OLA) and Underpinning Contract (UC).	Incident Coordinator
SO 2.8.2	Assigned Incident Analyst available?	External circumstances (for example, end of work shift, illness, or holiday) could cause an assigned Incident Analyst to become unavailable.	Incident Coordinator
SO 2.8.3	Reassignment required?	If yes, go to SO 2.2.3. If no, go to SO 2.8.4.	Incident Coordinator
SO 2.8.4	Applicable OLA or UC breached?	If yes, start the Incident Escalation process (SO 2.6). If no, go to SO 2.8.5.	Incident Coordinator
SO 2.8.5	Expected OLA/UC breach within 1 hour?	If yes, go to SO 2.8.6. If no, go to SO 2.8.8.	Incident Coordinator
SO 2.8.6	Get status update from Incident Analyst and vendor (if applicable)	Contact the assigned Incident Analyst to receive a status update of the incident. If the incident is reported to a vendor, contact the vendor for a status update.	Incident Coordinator
SO 2.8.7	Will the incident be solved on time?	The Incident Coordinator estimates whether or not the incident can still be resolved on time. If yes, go to SO 2.8.4. If no, go to SO 2.6.7 to escalate the incident immediately.	Incident Coordinator
SO 2.8.8	Expected OLA/UC breach within 4 hours?	Does the incident need to be resolved within 4 hours to reach the OLA/UC target date/time? If yes, go to SO 2.8.9. If no, go to SO 2.8.11.	Incident Coordinator
SO 2.8.9	Get status update from Incident Analyst and vendor (if applicable)	Contact the assigned Incident Analyst to receive a status update of the incident. If the incident is reported to a vendor, contact the vendor for a status update.	Incident Coordinator
SO 2.8.10	Take follow-up actions if required	The Incident Coordinator determines whether follow-up actions are required to resolve the incident according to the OLA/UC. If required, the Incident Coordinator performs the required actions.	Incident Coordinator
SO 2.8.11	Expected OLA/UC breach within 1 day?	If yes, go to SO 2.8.12. If no, go to SO 2.8.14.	Incident Coordinator
SO 2.8.12	Get status update from Incident Analyst and vendor (if applicable)	Contact the assigned Incident Analyst to receive a status update of the incident. If the incident is reported to a vendor, contact the vendor for a status update.	Incident Coordinator
SO 2.8.13	Take follow-up actions if required	The Incident Coordinator determines whether follow-up actions are required to resolve the incident according to the OLA/UC. If required, the Incident Coordinator performs the required actions.	Incident Coordinator
SO 2.8.14	Incident closed?	If yes, no further action is required. If no, go to SO 2.8.4.	Incident Coordinator

Complaint Handling (process SO 2.9)

Complaint Handling is the process by which the Service Desk Manager handles complaints. The Complaint category is typically used to indicate less than satisfactory service received by a user in the support or service delivery categories.

When the Service Desk Manager receives assigned incidents in the Incident or To Do queue, the manager accepts the incident. The manager investigates the cause of the complaint by evaluating the relevant information and talking to the people involved. The manager searches for an answer or solution to satisfy the user who filed the complaint, updates the incident ticket with the agreed on details, and then closes the incident ticket. You can see the details of this process in the following figure and table.

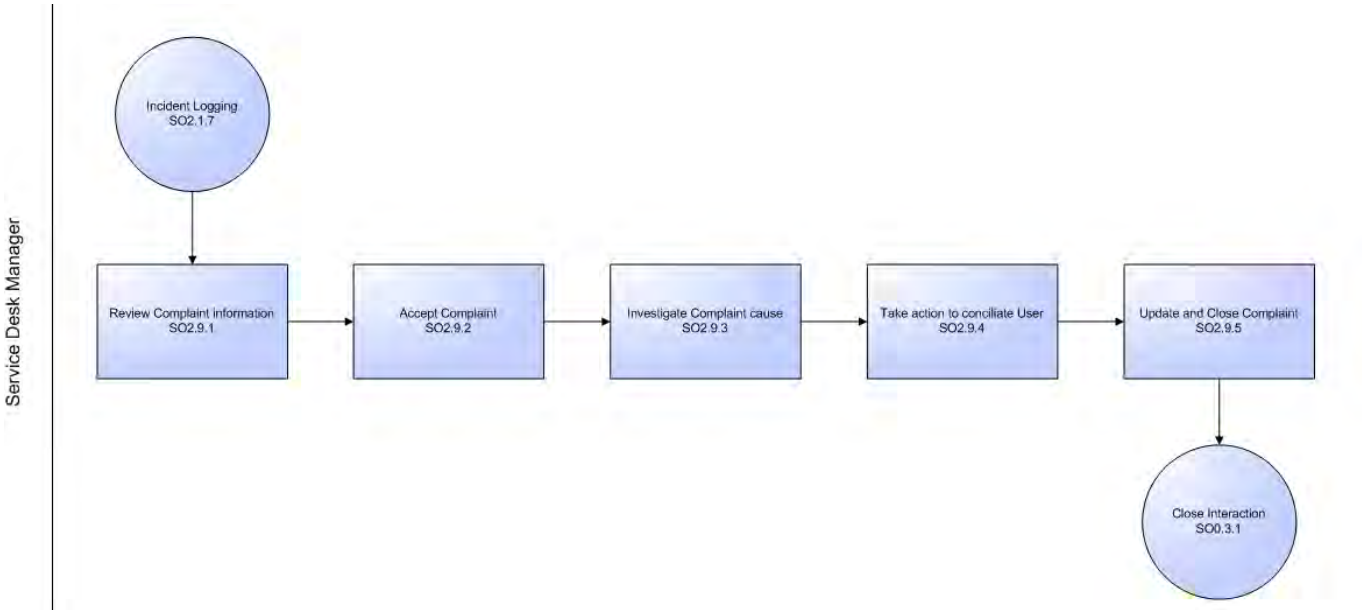

Figure 6-9 Complaint Handling workflow

Table 6-9 Complaint Handling process

Process ID	Procedure or Decision	Description	Role
SO 2.9.1	Review complaint information	The Service Desk Manager monitors the incident queue and reviews assigned incidents. The Service Desk Manager checks the contents of the complaint.	Service Desk Manager
SO 2.9.2	Accept complaint	The Service Desk Manager accepts the incident ticket to investigate the cause of the complaint.	Service Desk Manager
SO 2.9.3	Investigate complaint cause	The Service Desk Manager investigates the cause of the complaint by looking at the relevant information and talking to the people involved. The Service Desk Manager also searches for an answer or solution to satisfy the user who filed the complaint.	Service Desk Manager
SO 2.9.4	Take action to conciliate user	The Service Desk Manager contacts the user to solve the user's issue and tries to reach an agreement.	Service Desk Manager
SO 2.9.5	Update and close complaint	The Service Desk Manager updates the incident ticket with the agreed on details and closes the incident ticket.	Service Desk Manager

7 Incident Management Details

HP Service Manager uses the Incident Management application to enable the Incident Management process. The main function of Incident Management is to monitor, track, and record calls and open incidents as necessary.

In Incident Management, an Incident Analyst investigates, diagnoses, and proposes solutions for incidents. The Incident Analyst escalates those incidents requiring a change to the Incident Coordinator.

This section describes selected Incident Management fields in the out-of-box Service Manager system.

Topics in this section include:

Incident form after escalation from Service Desk

The Incident Coordinator reviews incidents escalated from the Service Desk and accepts or rejects each incident. The Incident Coordinator then assigns the incident to an Incident Analyst for investigation and diagnosis.

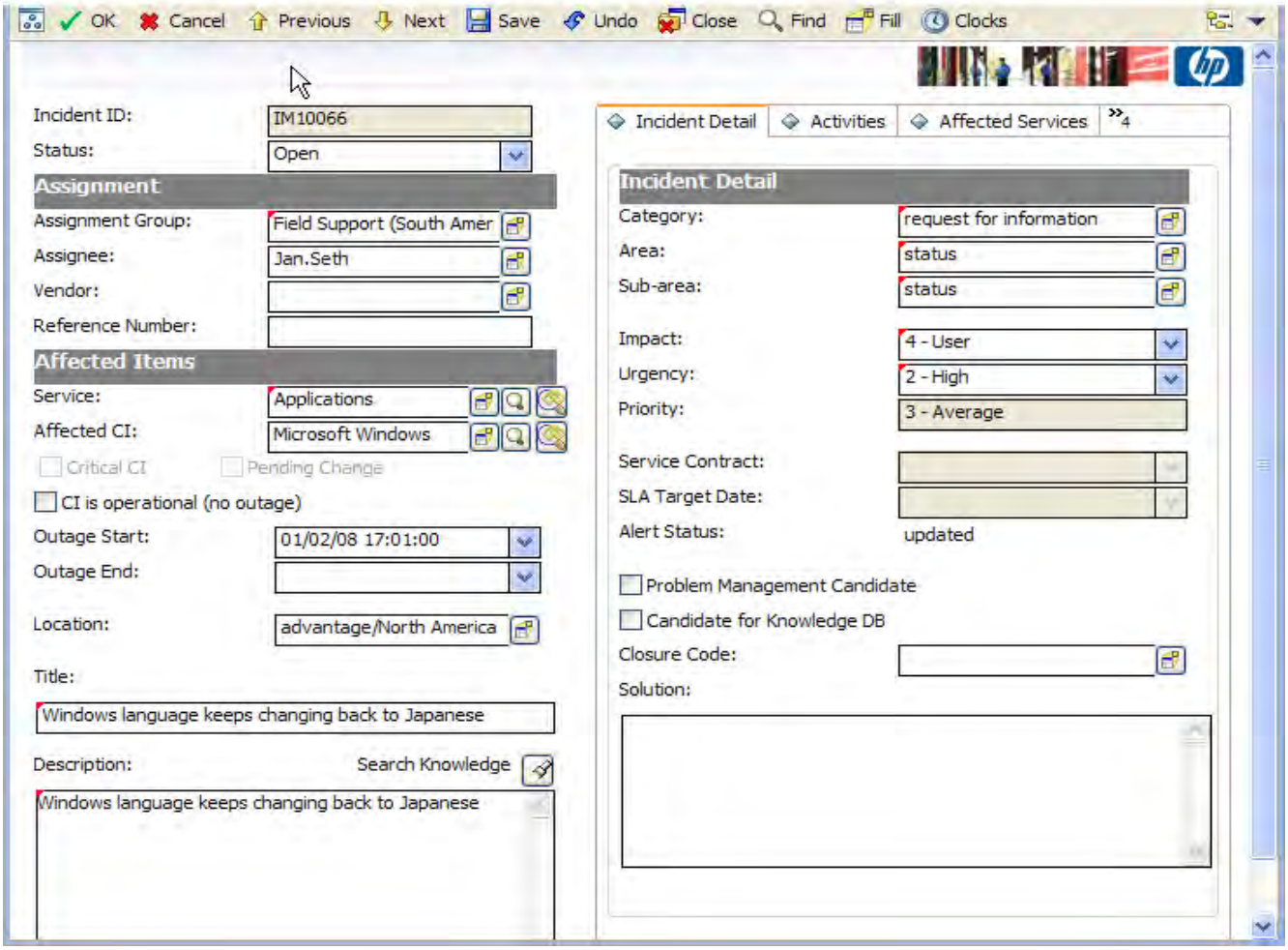

Figure 7-1 Incident escalated from Service Desk

Update incident form

The Incident Coordinator uses the update incident form to review the information and then assign the incident to an Incident Analyst in the appropriate support group. The Incident Analyst uses the incident update form to analyze the issue and determine if the incident can be resolved, and then updates the form accordingly. The Incident Manager uses the update incident form to monitor Service Level Agreement (SLA) compliance, to initiate escalation actions, or to register an emergency change request. The fields and tabs available for updating depend upon the assigned user role, assignment group, and the status of the incident.

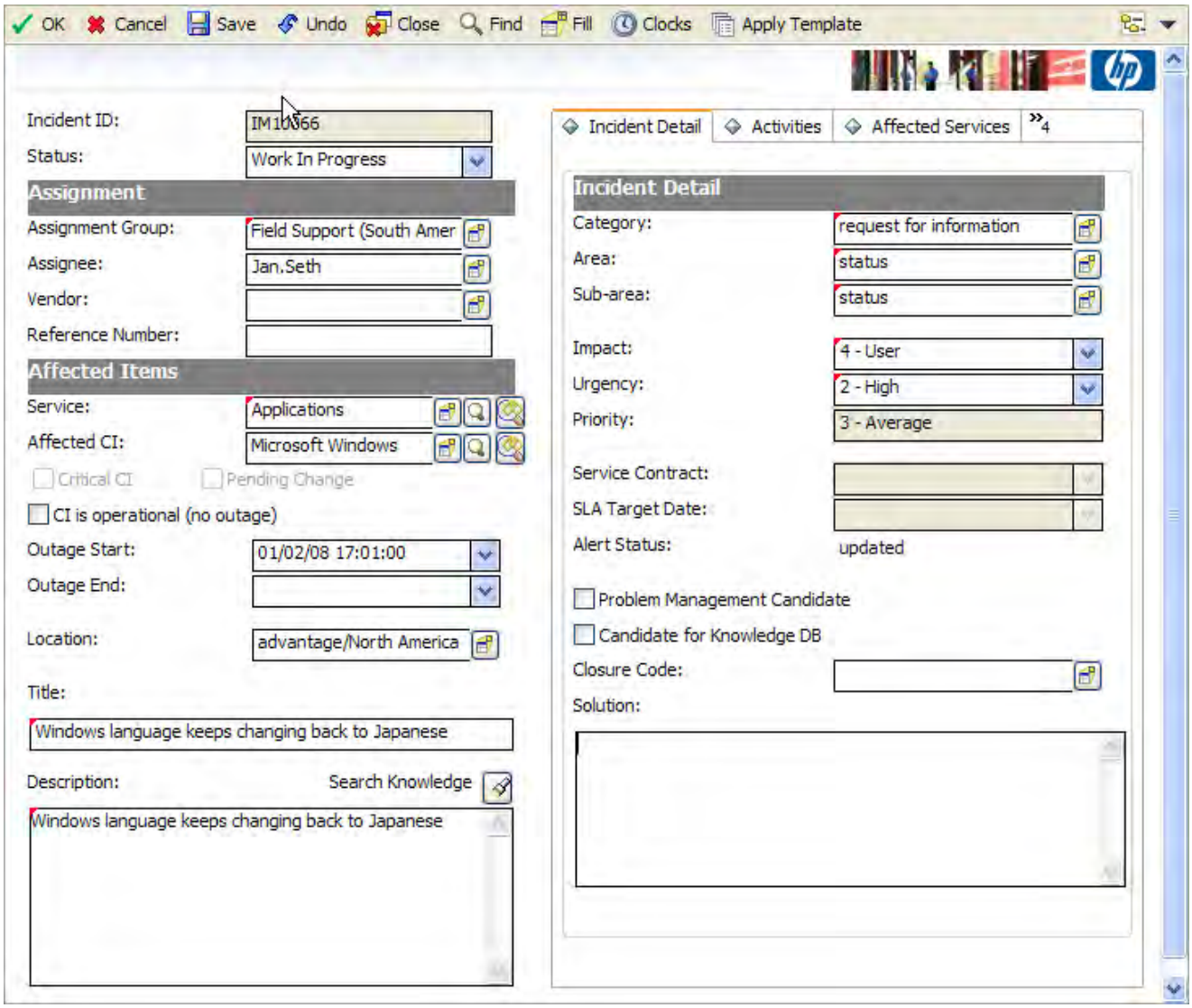

Figure 7-2 Update an incident form

Incident Management form details

The following table identifies and describes some of the features on the Incident Management forms.

When setting up events or web services to create incidents automatically, you must be sure to include all required fields for the incident.

Table 7-1 Incident Management form details

Label	Description
Incident ID	The system-generated unique ID for this incident.
Status	Displays the status of the incident. These statuses are available out-of-box: Note: The bold values are new values in Service Manager 7.l0. • Open — The incident that has been opened but it is not currently being worked on. • Closed — The incident has been resolved and the customer agrees. • Pending Other — You need something from an outside source other than customer or vendor • Resolved — There is a resolution, but it has not yet been verified by the customer • **Accepted** — You accept responsibility for the ticket. • Rejected — Someone else is responsible for the ticket. • Work In progress — The incident is being addressed. • Pending Customer — You need more information from the customer • Pending Vendor — You need something from the vendor • **Pending Change** — There is a related emergency change open; awaiting the close of that change. • Suspended — Customer has agreed to suspend the incident for a time; the ticket will not appear in your Inbox for that period.
Assignment Assignee	The name of the person assigned to work on this incident. This person is a member of the assigned support group. Assignees may belong to one or multiple assignment groups, based on the needs of your company.
Assignment Vendor	The name of the vendor the incident is assigned to. Used when a vendor needs to be involved in fixing the incident.
Assignment Reference Number	This number refers to the incident number from the vendor's logging system. This is an informational field for reference only.

Table 7-1 Incident Management form details (cont'd)

Label	Description
Assignment Assignment Group	The support group assigned to work on this incident. The service specified in the interaction form determines which default assignment group the system assigns to incidents that were escalated from interactions. An administrator assigns the default assignment group for a service on the Configuration Item (CI) detail form for the CI. When you search for the service in Configuration Management (Configuration Management > Resources > Search CIs), you see the default assignment group for the service specified in the Config admin group field. When you escalate an interaction to an incident, the assignment group is prepopulated, based on the service selected in the interaction. You can change the assignment group, if necessary. If you use the escalation wizard, assignment has both default and allowed groups as defined for the service, as well as the default group for the CI, if one has been registered. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. Tip: You may want to adapt the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager This is a required field.
Affected Items Service	The service affected by this incident. This field is populated with data from the interaction record. See User Interaction Management form details on page 44 for additional information. This is a required field.
Affected Items Affected CI	The configuration item (CI) that is affecting the service negatively. This field is populated with data from the interaction record. See User Interaction Management form details on page 44 for additional information.
Affected Items Critical CI	If selected (set to true), indicates that the affected Configuration Item (CI) is critical to normal operations. If the CI you specify has been marked as a critical CI by an administrator, the system marks this check box. You cannot modify this field on the incident form. It can only be changed by modifying the applicable CI device record.
Affected Items Pending Change	If the CI you select has been marked as Pending Change in the Configuration Management device record, the system marks this check box. This field indicates that there is a change pending for this CI. You cannot modify this field on the incident form. It can only be changed by modifying the applicable CI device record.

Table 7-1 Incident Management form details (cont'd)

Label	Description
Affected Items CI is operational (no outage)	If selected (set to true), indicates that the item is currently operational and that there is no outage. By default when you open an incident against a CI, the CI is flagged as down. If the CI is still working, you should mark this field.
Affected Items Outage Start	The date and time when the outage started. The outage start and outage end times are used to measure availability for the Service Level Agreements (SLAs). If the CI is flagged as down, availability SLAs start counting against the CI. The availability value defaults to the incident open and close times, but you should change this to report the actual outage start and end times because it may be several minutes or hours before the incident is opened or closed. For example, the device may have gone down in the night and the incident is not opened until someone reports the problem. In this case, the default open time does not accurately reflect the outage time.
Affected Items Outage End	The date and time of when the outage ended. The outage start and outage end times are used to measure availability for the SLAs. If the CI is flagged as down, availability SLAs start counting against the CI. The availability value defaults to the incident open and close times, but you should change this to report the actual outage end times. For example, the CI may become operational after it is restarted, but it may take several minutes or hours for someone to update the record to report that the incident is closed. In this case, the default close time does not accurately reflect the actual outage time.
Location	The location for which the incident has been reported. This field is prepopulated with data from an escalated interaction. The field is for informational purposes only. Location data is customer and implementation specific.
Title	A short description summarizing the incident. This field is prepopulated with data from an escalated interaction. This is a required field.
Description	A detailed description of the incident. This field is prepopulated with data from an escalated interaction. This is a required field.
Incident Detail > Category	This field describes the type of incident, based on ITIL service-centric processes. This field is prepopulated with data from the escalated interaction. For incidents assigned to them, the Incident Coordinator, Incident Manager, and Incident Analyst can update this field and the related area and subarea fields, if required. The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44 and Interaction categories on page 50.
Incident Detail > Area	This field is prepopulated with data from an escalated interaction. The area selections depend on the category. The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44 and Interaction categories on page 50.

Table 7-1 Incident Management form details (cont'd)

Label	Description
Incident Detail > Sub-area	The third level of classifying an interaction, mainly used for reporting purposes. This field is prepopulated with data from an escalated interaction. Service Manager displays different lists of subareas, depending on the area selected. For more information on categories and the areas and subareas associated with them, see Interaction categories on page 50. This is a required field. The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44.
Incident Detail > Impact	This field is prepopulated with data from an escalated interaction. It specifies the impact the incident has on the business. The impact and the urgency are used to calculate the priority. These impacts are available out-of-box: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User
Incident Detail > Urgency	This field is prepopulated with data from an escalated interaction. The urgency indicates how pressing the incident is for the organization. The urgency and the impact are used to calculate the priority. For additional information, see User Interaction Management form details on page 44.
Incident Detail > Priority	The order in which to address this incident in comparison to others. The priority value is calculated using initial impact and urgency. This field only appears for incidents being updated or escalated from interactions.
Incident Detail > Service Contract	Specifies the contract covering the affected equipment. This field is populated, based on the Service Level Agreement (SLA) information. The SLA records contain service contract information so when an SLA applies to an incident, the service contract is also populated according to the SLA. Note: In the current out-of-box system, no SLAs are defined with a Service Contract. Therefore, no out-of-box values are available for this field. Service contracts are financial agreements that define the services to be provided and the financial implications of using those services. This information is used to: Charge the customer for costs incurred while working with incidents, handling service desk interactions, or implementing changes to a specific service contract. Link discrete incidents and interactions to service contracts to provide up-to-date information about the state of each contract, including its budgeted allocations and the actual number of interactions and incidents applied against each contract. Associate service contracts with time and materials expended through Service Desk, Incident Management, and Change Management to compute the real cost of handling each incident and service desk interaction, as well as to calculate the cost of managing each service contract.

Table 7-1 Incident Management form details (cont'd)

Label	Description
Incident Detail > SLA Target Date	The date and time when the next Service Level Objective (SLO) expires. This field is populated based on the SLOs that match the incident information. The date used is the closest SLO to a breach before the agreement is breached. For example, if there are two SLOs for that incident and one expires in one hour and the other expires in one week, this field contains the value of current time+1hr. This field is the same as the Next Expiration field that appears on the SLA notebook tab.
Incident Detail > Alert Status	This system-generated field displays the alert status of the incident as it progresses through the processing stages. These alert statuses are available out-of-box: • open • updated • closed • reopened • resolved Note for legacy users: Alert stage 1, 2, 3, and Deadline alert are calculated based on the category settings. In the out-of-box system, these calculations are not configured. If you enable category-based alerts, you see these additional values: • alert stage 1 • alert stage 2 • alert stage 3 • DEADLINE ALERT
Incident Detail > Problem Management Candidate	If selected (set to true), this field indicates that the issue that caused the incident is most likely a problem. When selected, either a problem ticket should have been created, or the incident should have been associated with other problems or known errors. This field is only enabled for users who have rights to mark incidents as problem candidates. This capability is specified on the Incident Management Security Profile form. For the out-of-box system, these profiles include Incident Analyst, Incident Coordinator, Incident Manager, and Operator. When the Problem Management Candidate field is checked for the incident, the incident ticket appears in the Problem Manager default view for incidents. The Problem Manager can then review the incident to decide whether or not to open a related problem. Examples of problem candidates include cases where several customers report the same issue or where an issue recurs repeatedly.

Table 7-1 Incident Management form details (cont'd)

Label	Description
Incident Detail > Candidate for Knowledge DB	This field is intended for customers who do not have the Knowledge Management (KM) module. If selected (set to true), this field indicates that the solution is useful for other incidents and should be stored in the knowledgebase. This field is used for Information Retrieval (the IR Expert core and protocore tables). When you close incidents marked as solution candidates, the candidate (protocore) file fills. Knowledge engineers examine these proposed solutions and promote them to the central knowledgebase (core), if applicable. The IR Expert is disabled out-of-box for the installations that have the KM module. Customers who do have the KM module can search in the incident library for an incident. If you have the rights, you can create a knowledge article from an existing incident.
Incident Detail > Closure Code	Specifies a predefined closure code to describe how the incident has been resolved. The out-of-box options in this field are based on customer reference data. Tip: You may want to tailor these options to match your business needs. These closure codes are available out-of-box: • Not Reproducible • Out of Scope • Request Rejected • Solved by Change/Service Request • Solved by User Instruction • Solved by Workaround • Unable to Solve • Withdrawn by User
Incident Detail > Solution	Provides a description of the solution for the incident.
Affected Services	This notebook tab provides a list of affected services for the incident ticket. When a configuration item for the incident is added or updated, a schedule record is created that runs a routine to update the list of affected services. If the incident ticket is locked, the routine reschedules the schedule record for 5 minutes later.
SLA > Response Time Objective	This notebook tab provides a list of response SLOs related to the incident. The information includes SLA title, status, SLO name, From and To specifications for the SLA, and Expiration. Similar information is available for interactions, problems, and changes.

Table 7-1 Incident Management form details (cont'd)

Label	Description
SLA > Uptime Objectives	This notebook tab displays uptime availability data for the SLOs related to the incident. The data displayed includes the following information: • Status • SLO name • Required Monthly Uptime (%) • Withdrawn by User • Current Uptime this Month (%) • Next Expiration • Affected CI • SLO ID Similar information is available for interactions, problems, and changes.
SLA > Max Duration Objectives	This notebook tab displays duration availability data for the SLOs related to the incident. The data displayed includes the following information: • Status • SLO name • Total outages this month • Average outage duration • Next expiration • Affected CI • SLO ID Similar information is available for interactions, problems, and changes.
SLA > Upcoming Alerts	This notebook tab displays all upcoming SLA alerts to help users prioritize the incidents needing attention. The data displayed includes the following information: • Alert name • SLO name • Alert time Note: For additional information, see the online Help topic, Service Level Agreement alerts.

8 Problem Management Overview

The HP Service Manager Problem Management application, referred to as Problem Management throughout this chapter, supports the entire Problem Management process. Problem Management provides comprehensive Problem Management that allows you to find, fix, and prevent problems in the IT infrastructure, processes, and services.

Problem Management prevents problems and their resulting incidents, eliminates recurring incidents, and minimizes the impact of those incidents that cannot be prevented. It maximizes system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.

This section describes how Problem Management implements the best practice guidelines for the Problem Management processes.

Topics in this section include:

Problem Management within the ITIL framework

Problem Management is addressed in ITIL's *Service Operation* publication. The document describes Problem Management as the process responsible for managing the lifecycle of all problems.

The main benefits of Problem Management are improved service quality and reliability. As incidents are resolved, information about their resolution is captured. This information is used to identify and quickly resolve future similar incidents, and then to identify and fix the root cause of those incidents.

Problem Management functions both reactively and proactively.

- Reactive Problem Management resolves situations related to incidents. Reactive Problem Management is generally executed as part of Service Operation, and is based on incident history.
- Proactive Problem Management identifies and solves issues and known errors, before incidents occur. It is generally driven as part of Continual Service Improvement.

By actively preventing incidents, instead of just reacting to them, an organization provides better service and higher efficiency.

Differences between Problem Management and Incident Management

Incident Management and Problem Management are separate processes, but they are closely related. Incident Management deals with the restoration of service to users, whereas Problem Management manages the lifecycle of all problems and is concerned with identifying and removing the underlying causes of incidents.

Problem Management application

The Problem Management application helps you to minimize the effects of incidents caused by errors in the IT infrastructure. Problem Management helps you to prevent these errors from recurring. With Problem Management, the appropriate people can identify known errors, implement workarounds, and provide permanent solutions. It enables you to identify errors in IT infrastructure, record them, track the history, find resolutions for them, and prevent their recurrence.

The Problem Management application helps your personnel to record resolutions and make them easily available to affected user groups, to react more quickly to issues related to incidents, and to proactively resolve issues before incidents occur. Over the long term, using Problem Management leads to a reduced volume of incidents as well as saved time and money.

Problem Management categories

Problem Management comes with a single out-of-box category for problem tickets and known error records, BPPM. The BPPM category ensures that the problem workflow automatically conforms to the ITIL workflow.

If your business needs require changes to the out-of-box Problem Management workflow, you can define new categories with unique phases, or you can make changes to the default category. Each new category you define gives you the opportunity to design a different workflow for a problem ticket.

If you define new categories, be sure to set a default category. Problem Management requires a category value when it searches for problem tickets or known error records. Choosing a default category ensures that an administrator will not have to manually add a category value to each legacy record.

Problem and known error tasks

Problem and known error tasks have a single out-of-box task category named Default. You can change it or add other task categories. You can define unique task categories for the tasks that you assign from a problem ticket. When you create a known error of problem task, the category field displays “Problem” not Default.

Problem Management alerts

The Problem Management application creates automatic alerts and notifications. For example, it creates notifications when a problem, task, or known error opens, the owner changes, or the status changes. It also escalates problems automatically when not addressed on pre-agreed schedules. The expected resolution date is based on several elements and discussed with the stakeholders.

Problem Management process overview

The Problem Management process includes the activities required to identify and classify problems, to diagnose the root cause of incidents, and to determine the resolution to related problems. It is responsible for ensuring that the resolution is implemented through the appropriate control processes, such as Change Management.

Problem Management includes the activities required to prevent the recurrence or replication of incidents or known errors. It enables you to form recommendations for improvement, maintain problem tickets, and review the status of corrective actions.

Proactive Problem Management encompasses problem prevention, ranging from the prevention of individual incidents (for example, repeated difficulties with a particular system feature) to the formation of higher level strategic decisions. The latter may require major expenditures to implement, such as investment in a better network. At this level, proactive Problem Management merges into Availability Management. Problem prevention also includes information given to customers for future use. This information reduces future information requests and helps to prevent incidents caused by lack of user knowledge or training.

A general overview of the Problem Management processes and workflows is depicted in Figure 8-1,below. They are described in detail in Problem Management Workflows on page 103.

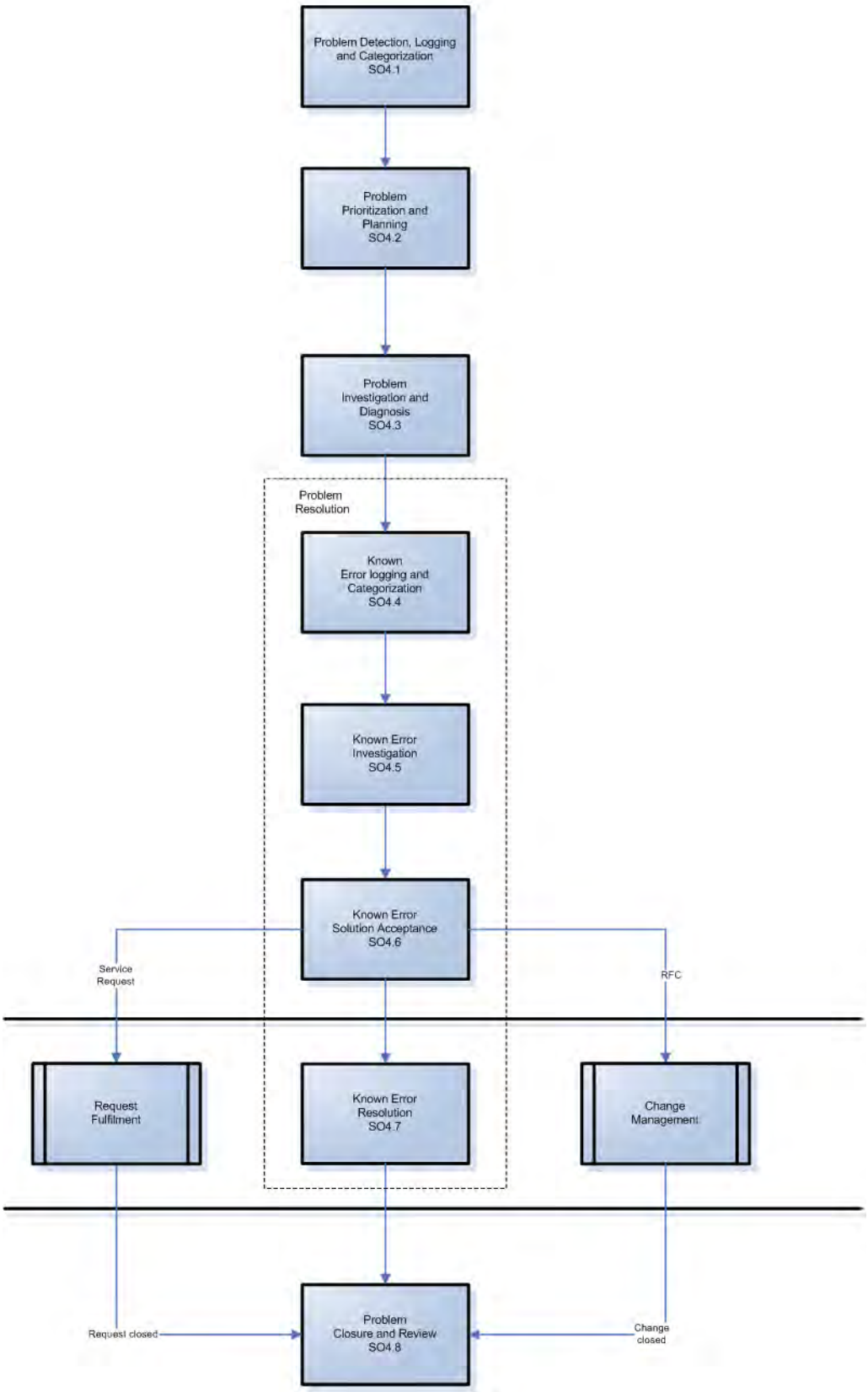

Figure 8-1 Problem Management process diagram

Problem Management phases

Problem Management phases are the activities in the life cycle of a problem. The phases represent the workflow steps within the process. ITIL includes all known error activities in one phase of Problem Management, the Problem Resolution phase. The Problem Management application brings more attention to Error Control as a process, and stores problems and known errors separately because of how they are commonly used.

- *Problem Control* identifies the problem. This workflow from the Problem Management shows how a problem moves through Problem Management. Each box represents a phase of the process.

Figure 8-2 Problem Control phases

- *Error Control*, which falls entirely under the Problem Resolution phase, identifies a solution that is then delivered by the Change Management application. This workflow from the Problem Management application shows how a known error moves through Problem Management. Each box represents a phase of the process.

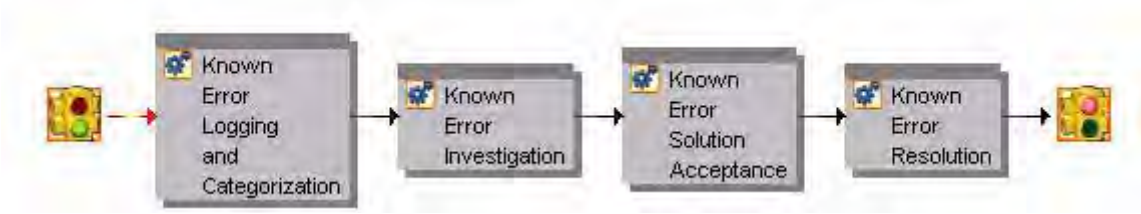

Figure 8-3 Error Control phases

The Problem Management phases listed below are described in detail in the Problem Management Workflows.

- Problem Detection, Logging, and Categorization (process SO 4.1) on page 103, includes the activities involved in finding and then describing the problem.
- Problem Prioritization and Planning (process SO 4.2) on page 107, includes the activities necessary to prioritize the problems, and to plan the investigation and resolution activities.
- Problem Investigation and Diagnosis (process SO 4.3) on page 109, includes the activities that identify the root cause of problems. **You can create problem tasks in this phase.** Each task belongs to a phase. All the tasks associated with a phase must be completed before the problem ticket can move to the next phase. A problem task is assigned to a person who is responsible for completing it.
- *Problem Resolution* includes all Error Control activities, from recording the known error to resolving it. Generally you can expect a one-to-one relationship between problems and known errors, but there can be exceptions. Service Manager allows more than one known error to be associated with a problem, and also allows multiple problems to be associated with a particular known error.
  - Known Error Logging and Categorization (process SO 4.4) on page 113, includes the activities necessary for creating and categorizing known error record.
  - Known Error Investigation (process SO 4.5) on page 116, includes the activities necessary for finding a temporary fix or permanent solution for the known error. You can create known error tasks in this phase. All of the tasks associated with a phase must be completed before moving to the next phase.

— Known Error Solution Acceptance (process SO 4.6) on page 119, includes the activities necessary for reviewing and approving the solution for implementation. You cannot close a known error if there is a related Change open. You can create a Change Request during this phase.

— Known Error Resolution (process SO 4.7) on page 122, includes the activities by which stakeholders can ensure that a fix for a known error is implemented.

You can only create a change request during the known error processes, not during the earlier Problem Management processes. It is only at that point that you have enough information to describe the change that must be made in order to resolve the problem.

- Problem Closure and Review (process SO 4.8) on page 125, includes the activities involved in determining whether the problem and all related known errors have been resolved, seeking improvements to the process, and preventing recurrence of incidents or mistakes.

Problem Management user roles

Table 8-1 describes the responsibilities of the Problem Management user roles.

Table 8-1 Problem Management user roles

Role	Responsibilities
Problem Manager	• Prioritize and plan problems registered by the Problem Coordinators. • Communicate with stakeholders if required. • Inform the Change Manager if required. • Defer problems if needed. • Decide on investigation of known errors. • Register Request for Changes or Service Requests to solve known errors. • Conduct problem review and document lessons learned. • Close problem and inform stakeholders. • Monitor the Problem and Known Error Resolution progress and perform required action.
Problem Coordinator	• Periodically perform analysis to see if new problems need to be registered. • Register problems. • Assign work to Problem Analysts and coordinate root cause analysis. • Register known errors. • Inform Problem Manager. • Assign known error to Problem Analyst. • Validate proposed solutions to known errors. • Validate outcome of closed changes and close known error. • Validate that a problem is solved.
Problem Analyst	• Investigate and diagnose assigned problems for workarounds and/or root causes. • Review and accept or reject assigned known errors. • Investigate and diagnose assigned known errors and propose solutions and workarounds. • Implement corrective actions and close known error.

Input and output for Problem Management

Problems can be triggered and resolved in several ways. Table 8-2 outlines the inputs and outputs for the Problem Management process.

Table 8-2 Input and output for Problem Management

Input to Problem Management	Output from Problem Management
• Incidents for which the cause is not known and/or incidents that are likely to recur (from incident Management) • Incidents that reveal that an underlying problem exists (for example, an application error or bug) • Notification from a supplier or product manager that a problem exists (for example, from a development team or supplier known error database) • Potential security breaches of products deployed in the IT environment (for example, from suppliers or security analysts). • Analysis of incident trends and history (that is, proactive Problem Management) • Incident Management — Incidents classified as problem candidates — Trend analysis and review of closed incidents (for which a workaround has been used to resolve the incident) — Incident reports (trends, summary) • Event management — Trend analysis and review of events (for example, performance events) — Error logs • Configuration management — Configuration details and relationships (service model) • Change management — RFC and change request status, approval and closure. • Security management — Notification of potential security breaches that require resolution. • Suppliers (external providers) • Notification of problems from suppliers/vendors.	• Problems • Known errors • Workarounds • Problem reports (for example, status updates, trends, and performance) Note: Information on workarounds, permanent fixes, or progress of problems should be communicated to those affected or required in order to support the affected services.

Key performance indicators for Problem Management

The Key Performance Indicators (KPIs) in Table 8-3 are useful for evaluating your Problem Management processes. In addition to the data provided by Service Manager, you may need additional tools to report all of your KPI requirements. To visualize trend information, it is useful to graph KPI data.

Table 8-3 Key Performance Indicators for Problem Management

Title	Description
Average time to diagnose	Average time to diagnose problems and pinpoint the root cause and the known error(s), in a given time period.
Average time to fix	Average time to fix known error(s).
Number of new problems	Total number of problems recorded, in a given time period.
Number of solved problems	Total number of problems solved, in a given time period.
Incidents caused by problems	The number of incidents occurring before the problem is resolved, in a given time period.

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included below.

ITIL V3 Key Performance Indicators

The following are ITIL V3 KPIs for Problem Management:

- Total number of problems recorded in the period (as a control measure)
- Percentage of problems resolved within SLA targets; percentage not resolved within SLA targets
- Number and percentage of problems that exceed target resolution times
- Backlog of existing problems and the trend (that is, static, reducing, or increasing)
- Average cost of handling a problem
- Number of major problems, including opened, closed, backlog
- Percentage of major problem reviews successfully performed s
- Number of known errors added to the known error Database (KEDB)
- Percentage accuracy of the KEDB (from audits of the database)
- Percentage of major problem reviews completed successfully and on time

COBIT 4.1 Key Performance Indicators

The following are the COBIT 4.1 KPIs for Problem Management:

- Number of recurring problems with an impact on the business
- Number of business disruptions caused by operational problems
- Percent of problems recorded and tracked
- Percent of problems that recur (within a time period), by severity
- Percent of problems resolved within the required time period

- Number of open/new/closed problems, by severity
- Average and standard deviation of time lag between problem identification and resolution
- Average and standard deviation of time lag between problem resolution and closure
- Average duration between the logging of a problem and the identification of the root cause
- Percent of problems for which a root cause analysis was completed
- Frequency of reports or updates to an ongoing problem, based on the problem severity

RACI matrix for Problem Management

A Responsible, Accountable, Consulted, and Informed (RACI) diagram or RACI matrix is used to describe the roles and responsibilities of various teams or people in delivering a project or operating a process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes.The RACI matrix for Problem Management is shown in Table 8-4.

Table 8-4 RACI matrix for Problem Management

Process ID	Activity	Problem Manager	Problem Coordinator	Problem Analyst	Change Coordinator
SO 4.1	Problem Detection, Logging, and Categorization	A/I	R		
SO 4.2	Problem Prioritization and Planning	A/R	C		
SO 4.3	Problem Investigation and Diagnosis	A	R	R	
SO 4.4	Known Error Logging and Categorization	A	R		
SO 4.5	Known Error Investigation	A	R		
SO 4.6	Known Error Solution Acceptance	A/R	C		
SO 4.7	Known Error Resolution	A	R	R	R
SO 4.8	Problem Closure and Review	A/R	C		
SO 4.9	Problem and Known Error Monitoring	A/R	C		

9 Problem Management Workflows

Problem Management includes the activities required to identify and classify problems, diagnose the root cause of incidents and to determine the resolution to related problems. It is responsible for ensuring that the resolution is implemented through the appropriate control processes, such as Change Management.

Problem Management includes the activities required to prevent the recurrence or replication of incidents or known errors. It enables you to form recommendations for improvement, maintain problem tickets, and review the status of corrective actions.

The Problem Management process consists of the following processes, which are included in this chapter:

Problem Detection, Logging, and Categorization (process SO 4.1)

The Problem Detection, Logging, and Categorization process starts when the Problem Coordinator determines that a problem ticket needs to be opened to investigate an existing or potential problem. This process may be started in response to a single incident or a series of related incidents, and it may also be the result of proactive investigation of a potential problem.

It should include reference to information that assists analysis, such as:

- Asset and Configuration
- Change Management
- Published known error and workaround information from suppliers
- Historical information about similar problems
- Monitoring event logs and data collected by system management tools

The incident(s) that initiated the problem ticket should be referenced, and relevant details copied from the incident ticket(s) to the problem ticket. The identified workaround or temporary fix as defined by the Incident Analyst is also captured, if available.

Details for this process can be seen in Figure 9-1 and Table 9-1.

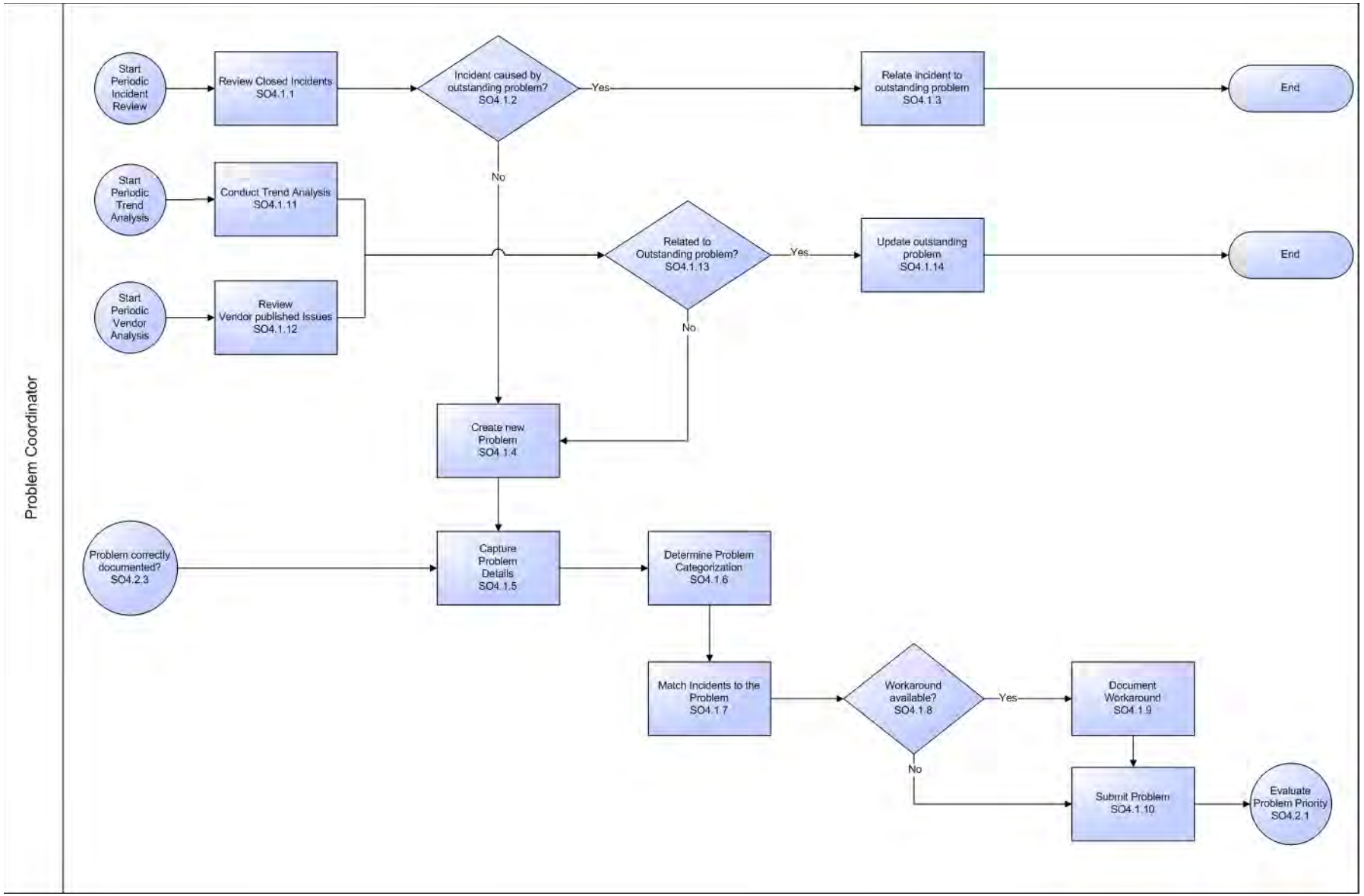

Figure 9-1 Problem Detection, Logging, and Categorization workflow

Table 9-1 Problem Detection, Logging, and Categorization process

Process ID	Procedure or Decision	Description	Role
SO 4.1.1	Review closed incidents	Periodically, the Problem Coordinator must review the closed incidents to detect new problems or match incidents to existing problems that have not been resolved. Analysis of incident data may reveal that similar or reoccurring incidents are reported, which means that a permanent fix must be found. Select incidents since last review by using the following criteria: • Major incidents (high impact) • Incidents resolved through a workaround or temporary fix not matched to a problem. • Suspected problems (as identified by stakeholders) • Candidates for problems All closed incidents not resolved through a permanent fix, temporary fix, or workaround need to be matched to existing problems, or a new problem must be created. Incident Management staff may already have linked incidents to existing problems (for example, if a workaround has been applied).	Problem Coordinator
SO 4.1.2	Incident due to an outstanding problem of known error?	Verify whether the incident is caused by an outstanding problem or known error. If yes, go to SO 4.1.3. If no, go to SO 4.1.4. It is important to link incidents to existing problems to monitor the number of reoccurring incidents. This helps you to identify problems that are not resolved. The incident count is the number of times that this particular problem has resulted in an incident, and is updated in the problem ticket. The incident count influences the prioritization by giving an indication of the frequency of occurrence and thus the impact this issue is having on the business.	Problem Coordinator
SO 4.1.3	Relate incident to outstanding problem	If the incident is caused by an outstanding problem, the incident must be linked to the problem ticket. If needed, the problem ticket is updated and the Problem Analyst is notified (for example, when a workaround has been applied).	Problem Coordinator
SO 4.1.4	Create new problem	If there is no previously established problem ticket, a new problem ticket is created (for example, based on the selected incident ticket). Details from the incident are copied to the problem ticket. A new problem can be created from a registered incident (reactively) or proactively by identifying problems and known errors before incidents occur.	Problem Coordinator

Table 9-1 Problem Detection, Logging, and Categorization process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 4.1.5	Capture problem details	After a problem is identified or detected, it must be accurately recorded. The Problem Manager fills out the problem details (some fields are copied from the related incident). A brief description and detailed description are added or updated to define the problem in more detail. The problem must be described in terms of symptoms and impact of the problem from a business perspective. Recording problem details consists of the following activities: • Determine affected service(s) and Configuration Items • Determine impact on the business • Provide an impact code and description • Determine model, version, or CI types that have this particular problem • Determine frequency of incident reoccurrence • Determine the specific conditions under which a service disruption may occur	Problem Coordinator
SO 4.1.6	Determine problem categorization	Determine the correct category for the problem ticket.	Problem Coordinator
SO 4.1.7	Match incidents to the problem	Search for incidents that are caused by this problem. Link these incidents to the new problem.	Problem Coordinator, Incident Mgmt Staff
SO 4.1.8	Workaround available?	Verify whether a workaround or fix is available based on incident history. If yes, go to SO 4.1.9. If not, go to SO 4.1.10.	Problem Coordinator
SO 4.1.9	Document workaround	Document the workaround captured from the related incident.	Problem Coordinator
SO 4.1.10	Submit problem	Review and complete the problem ticket details, including a description. Save the problem ticket and update the problem phase to Problem Prioritization, Assignment, and Scheduling. Service Manager then selects a default priority, based on the impact and urgency code. After that, update the phase to Problem Prioritization and Planning, and continue with activity Evaluate Problem Priority SO 4.2.1.	Problem Coordinator
SO 4.1.11	Conduct trend analysis	Review event and monitoring data (for example, performance and availability trends). Identify potential problems, such as capacity and performance issues. Analyze the data provided by availability, capacity, and security management to determine potential problems.	Problem Coordinator

Table 9-1 Problem Detection, Logging, and Categorization process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 4.1.12	Review vendor published issues	Review information from suppliers periodically to identify problems and known errors (that is, the known errors discovered and published by providers). An example of such an item is a known security breach.	Problem Coordinator
SO 4.1.13	Related to outstanding problem?	After a potential problem has been detected through trend analysis or information provided by suppliers and development teams, determine if the issue has already been recorded as a problem or a known error. If yes, go to SO 4.1.14. If no, continue with SO 4.1.4.	Problem Coordinator
SO 4.1.14	Update outstanding problem	Update problem ticket (and any related known errors) with information and details captured from suppliers and other sources. After the update, the stakeholders and responsible Problem Analyst may need to be informed of new insights.	Problem Coordinator

Problem Prioritization and Planning (process SO 4.2)

The Problem Prioritization and Planning process gives you the opportunity to establish the priority of the problems and to plan resolution activities, such as setting deadlines for root cause analysis, solution investigation, and resolution target dates.

Prioritize problems based on impact and urgency in the same way that you prioritize incidents but take severity into account as well.

- *Impact* is based on the scale of actual or potential damage to the customer's business.
- *Urgency* is based on the time between the problem or incident being detected and the time that the customer's business is impacted.
- *Severity* is based on how serious the problem is from an infrastructure perspective as well as the frequency and impact of related incidents. For example, how extensive is the problem (how many CIs are affected)?

Discuss the problem with the stakeholders during a problem meeting decide whether to assign resources (with associated costs) and target dates to investigate the problem. Base the targets for resolution on priority level. Consider the following factors when scheduling the resolution of problems:

- Priority
- Skills available
- Competing requirements for resources
- Effort or cost to provide the method of resolution
- Duration of time to provide a method of resolution

Details for this process can be seen in Figure 9-2 and Table 9-2.

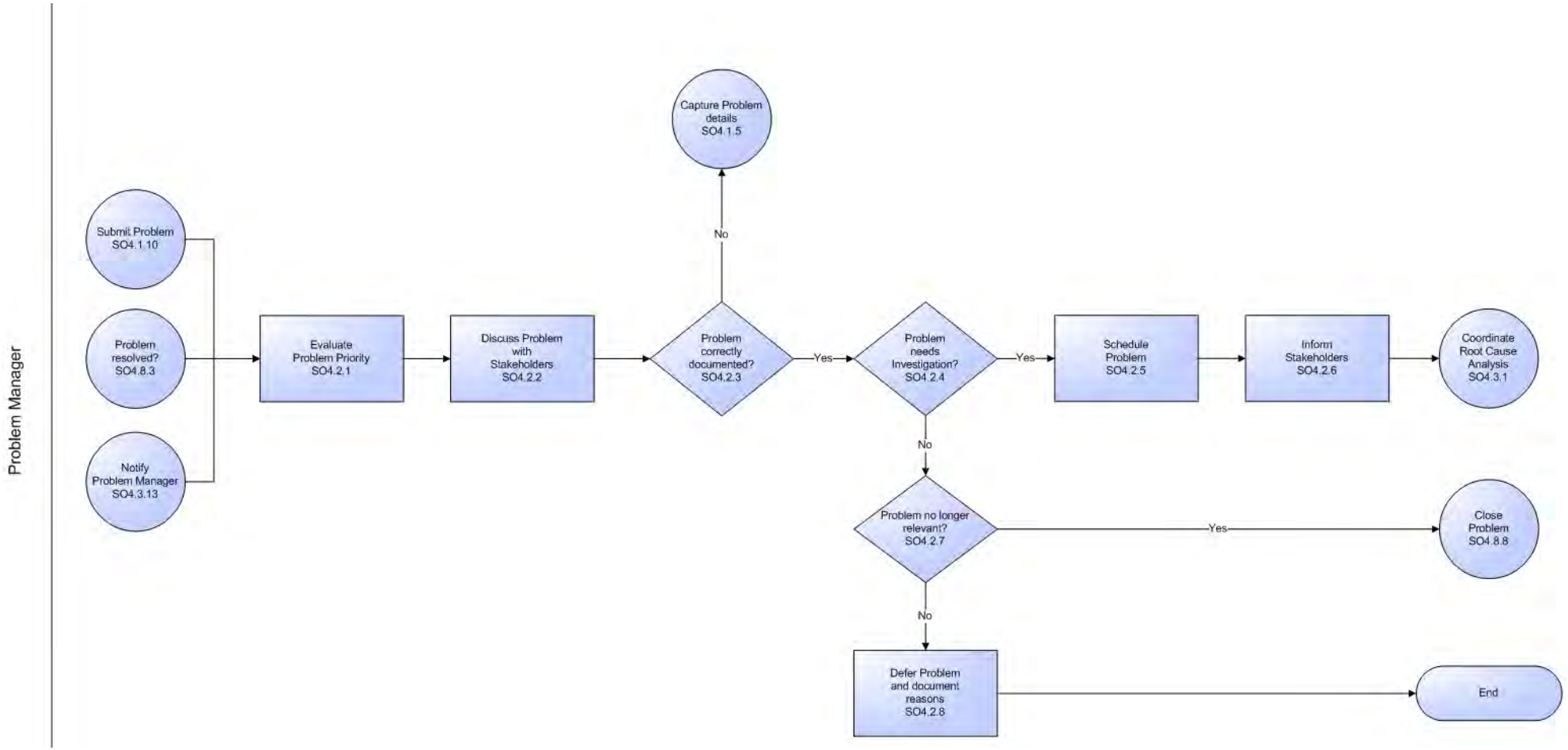

Figure 9-2 Problem Prioritization and Planning workflow

Table 9-2 Problem Prioritization and Planning process

Process ID	Procedure or Decision	Description	Role
SO 4.2.1	Evaluate problem priority	The problem priority is evaluated based on the impact, urgency, severity, frequency and risk. For example, the frequency of reoccurring incidents may influence the urgency to resolve the problem; also a risk assessment may be required. Due to resource constraints, it is important to focus on those problems that have the highest impact on the business (for example, service availability, risks, and customer satisfaction).	Problem Manager
SO 4.2.2	Discuss problem with stakeholders	Discuss the problem with stakeholders during a problem meeting to agree on the priority of resolving the problem.	Problem Manager
SO 4.2.3	Problem correctly documented?	Based on the review with stakeholders, determine whether the problem is correctly documented and categorized. If yes, continue with activity SO 4.2.4. If no, go back to activity SO 4.1.5 to update the problem details.	Problem Manager
SO 4.2.4	Problem needs investigation?	After reviewing the problem with stakeholders, determine whether to continue with the problem investigation or defer the problem. If you want to continue with the problem investigation, go to SO 4.2.5. If not, go to SO 4.2.7.	Problem Manager
SO 4.2.5	Schedule problem	Determine the target dates for the problem milestones. Target dates are determined based on the priority and impact on affected services. This planning also considers whether an effective workaround or fix is available. The problem is assigned to the responsible group. Update problem to next phase Problem Investigation and Diagnosis.	Problem Manager
SO 4.2.6	Inform stakeholders	Inform the stakeholders of the planning and resources assigned to investigate the problem. Update the Problem Coordinator about the problem.	Problem Manager
SO 4.2.7	Problem no longer relevant?	Determine whether to close the problem or to defer the problem for a specified period of time (for example, to review the problem at a later phase). It is possible that no effort is currently planned to investigate the problem (for example, if the likelihood of recurrence is low). If the problem is not recognized as being an issue by stakeholders, close the problem and document the reason. Update the problem phase to Problem Closure and Review, and then continue with SO 4.8.8. If the problem is still relevant, continue with SO 4.2.8.	Problem Manager
SO 4.2.8	Defer the problem and document reason	Defer the problem for a specified period of time. Document the reason and update the status of the problem to deferred status. Periodically the Problem Manager reviews the deferred problems to determine appropriate actions.	Problem Manager

Problem Investigation and Diagnosis (process SO 4.3)

The Problem Investigation and Diagnosis process helps identify the root cause of the problem. Where appropriate, Problem Management should develop and maintain workarounds to enable Incident Management to help service restoration. Different specialists can be involved for this root cause analysis. If necessary, refer to external resources to verify whether the problem has already been identified and published by vendors. Details for this process can be seen in Figure 9-3 and Table 9-3.

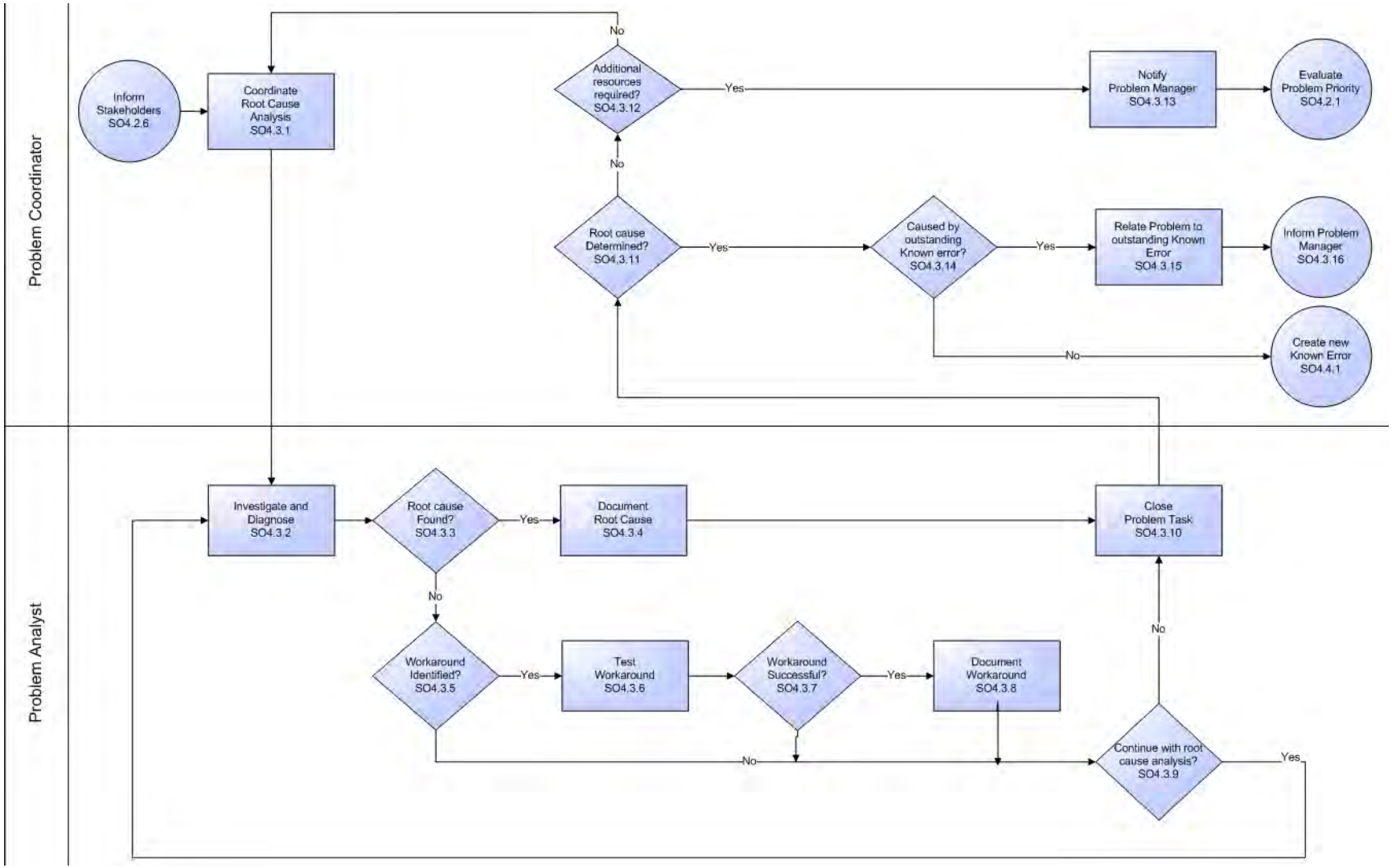

Figure 9-3 Problem Investigation and Diagnosis workflow

Table 9-3 Problem Investigation and Diagnosis process

Process ID	Procedure or Decision	Description	Role
SO 4.3.1	Coordinate root cause analysis	Determine the required skills and resources to investigate the problem. Create and assign problem tasks to Problem Analyst(s) responsible for root cause analysis. The due date for the assigned task is filled in by the Problem Coordinator. Additional resources can be used for this analysis (for example, contact suppliers and other specialists). Monitor the outstanding problem tasks.	Problem Coordinator
SO 4.3.2	Investigate and diagnose	The Problem Analyst reviews the problem task, and investigates and diagnoses the problem. Determine workaround and find the root cause.	Problem Analyst
SO 4.3.3	Root cause found?	If yes, continue with SO 4.3.4. If no, go to SO 4.3.5.	Problem Analyst
SO 4.3.4	Document root cause	Document the root cause in the problem task. The problem task can be closed and the Problem Coordinator informed about the progress. Continue with SO 4.3.10.	Problem Analyst
SO 4.3.5	Workaround identified?	If yes, continue with SO 4.3.6. If no, continue with SO 4.3.9.	Problem Analyst
SO 4.3.6	Test workaround	Test the identified workaround to validate the suitability for resolving related incidents.	Problem Analyst
SO 4.3.7	Workaround successful?	If yes, go to SO 4.3.8. If no, go to SO 4.3.9.	Problem Analyst
SO 4.3.8	Document workaround	Update the workaround (in the known error and problem ticket) and inform stakeholders.	Problem Analyst
SO 4.3.9	Continue with root cause analysis?	The Problem Analyst determines whether he or she has the capabilities to investigate and determine the root cause of the problem (that is, skill level and available time). If yes, continue with SO 4.3.2. If no, go to SO 4.3.10.	Problem Analyst
SO 4.3.10	Close problem task	The Problem Analyst closes the task and documents the results. If applicable, the Problem Analyst also documents the reasons a root cause is not found. If the Problem Analyst cannot find the root cause he or she closes the task. Continue with activity SO 4.3.11.	Problem Analyst
SO 4.3.11	Root cause determined?	The Problem Coordinator validates the results of the problem task. If the root cause is determined, continue with SO 4.3.14. If not, go to SO 4.3.12 and determine whether additional resources are needed or if escalation is required.	Problem Coordinator
SO 4.3.12	Additional resources required?	Determine whether additional resources are needed to investigate the cause of the problem. If yes, go to SO 4.3.13. If no, continue with SO 4.3.1.	Problem Coordinator
SO 4.3.13	Notify Problem Manager	Escalate to the Problem Manager. Inform the Problem Manager that additional resources are needed to resolve the problem and modify the phase of the problem to the previous phase (Problem Prioritization and Planning). Continue with SO 4.2.1.	Problem Coordinator

Table 9-3 Problem Investigation and Diagnosis process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 4.3.14	Caused by outstanding known error?	Determine whether the root cause for this problem is related to an outstanding known error. If yes, continue with SO 4.3.15. If no, forward the problem to the Problem Resolution phase, and then create a new known error record (see procedure SO 4.4.1).	Problem Coordinator
SO 4.3.15	Relate problem to outstanding known error	The problem is moved to the Problem Resolution phase and linked to the existing known error record. The resolution of the problem is dependent on the resolution of this known error (already assigned to a Problem Coordinator).	Problem Coordinator
SO 4.3.16	Inform Problem Manager	Inform the Problem Manager of the root cause and any dependency with another known error record. The resolution of the problem is dependent on the outstanding known error.	Problem Coordinator

Problem Resolution (known error processes)

After the Problem Management Investigation and Diagnosis phase has identified the root cause of an incident, the Problem Resolution phase starts. The Problem Resolution phase includes known error activities, from creating to finding a solution for a known error.

The known error processes are as follows:

- Known Error Logging and Categorization (process SO 4.4) on page 113
- Known Error Investigation (process SO 4.5) on page 116
- Known Error Solution Acceptance (process SO 4.6) on page 119
- Known Error Resolution (process SO 4.7) on page 122

The known error activities are discussed in detail in each of the known error processes.

Known Error Logging and Categorization (process SO 4.4)

The known Error Logging and Categorization process includes the creation of known error records and the elaboration of the description of the underlying cause and possible workaround (if identified).

All known errors should be recorded against the currently and potentially affected services in addition to the configuration item (CI) suspected of being at fault. Information on known errors in services being introduced into the live environment should be recorded in the knowledgebase, together with any workarounds. A known error should not be closed until after it has been resolved successfully.

The customer or service provider may decide that the resolution is too expensive or not beneficial to the business. In this case, the problem or known error is deferred. The reasons for deferred resolution should be clearly documented. The known error record should remain open, since new incidents are likely to occur and may require workarounds or a reassessment of the decision to resolve.

If the problem is caused by more than one error (for example, both an application and an infrastructure error), multiple known errors can be created.The Problem Manager reviews the known error and determines the planning for the solution investigation and resolution. If an effective workaround is identified, the known error has a lower priority, and the resolution may be deferred for a specified period of time.

Details for this process can be seen in Figure 9-4 and Table 9-4.

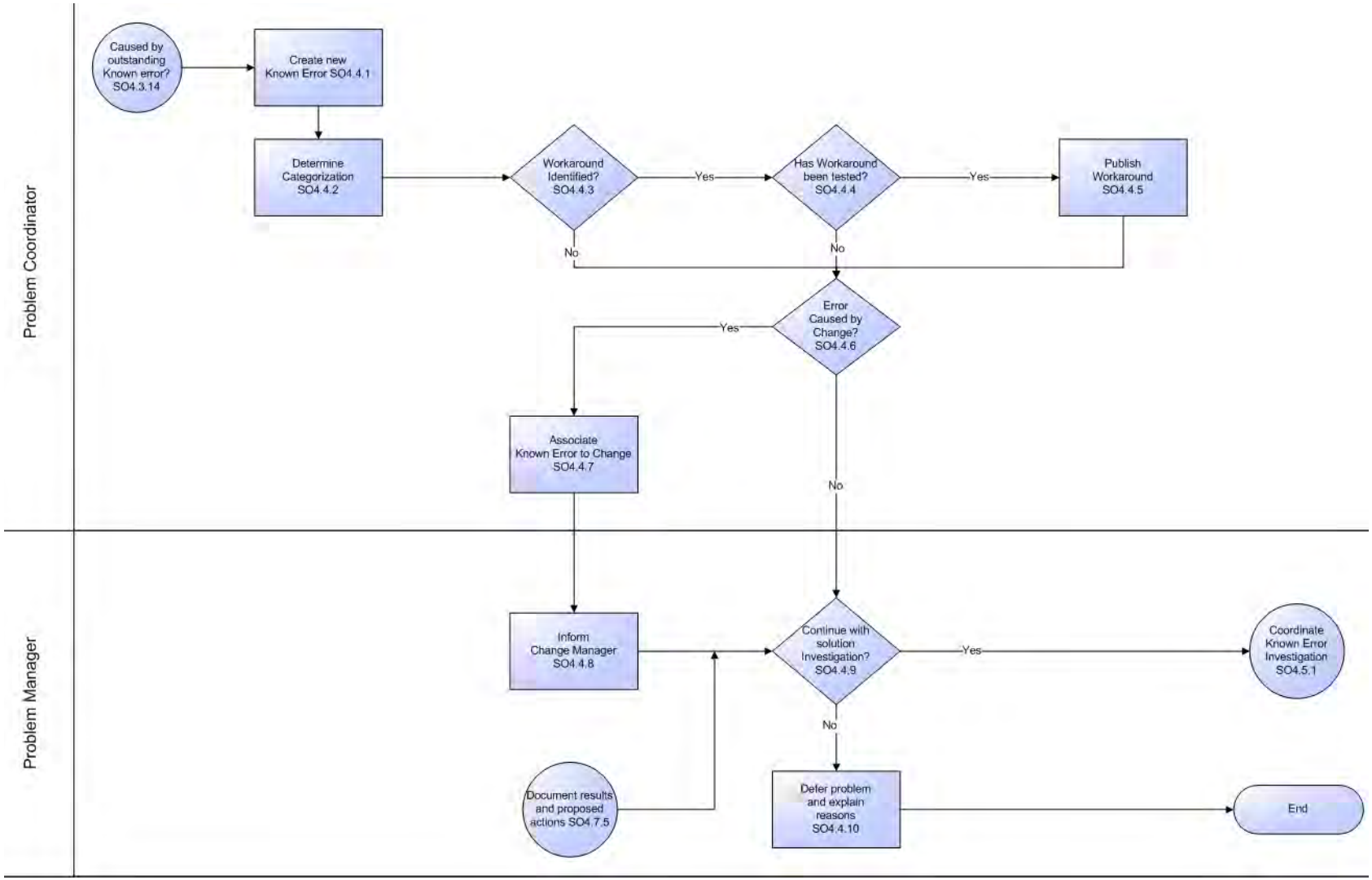

Figure 9-4 Known Error Logging and Categorization workflow

Table 9-4 Known Error Logging and Categorization process

Process ID	Procedure or Decision	Description	Role
SO 4.4.1	Create new known error	After the problem has been successfully diagnosed, a new known error record is created by using details from the problem ticket. Document the known error details, including the root cause and CIs that are at fault.	Problem Coordinator
SO 4.4.2	Determine categorization	Capture the categorization of the root cause, which is initially copied from the problem ticket.	Problem Coordinator
SO 4.4.3	Workaround identified?	If applicable, a temporary workaround is also documented. If a workaround is identified, continue with SO 4.4.4. If not, continue with SO 4.4.6.	Problem Coordinator
SO 4.4.4	Has the workaround been tested?	Validate whether the workaround has already been tested. If tested, continue with SO 4.4.5. If not, continue with SO 4.4.6.	Problem Coordinator
SO 4.4.5	Publish workaround	Update the workaround documented in the known error and problem ticket, and inform stakeholders.	Problem Coordinator
SO 4.4.6	Error caused by a change?	Validate whether the error is introduced or caused by a recently implemented change or release (that is, errors resulting from a change or incorrectly applied change). Note: Errors are often caused by incorrectly applied changes. If the error is introduced by a recently applied change, the change may need to be undone or reopened. If the error is caused by a change, continue with SO 4.4.7. If not, continue with SO 4.4.9.	Problem Coordinator
SO 4.4.7	Associate known error to a change	Relate the root cause to the original change that caused the problem.	Problem Coordinator
SO 4.4.8	Inform Change Manager	Inform the Change Manager and determine corrective actions, such as undoing or redoing the change. Depending on the result of undoing or redoing the change, the solution investigation continues.	Problem Manager
SO 4.4.9	Continue with solution investigation	Determine whether the known error must be investigated in more detail to find a solution or workaround. If the known error requires further investigation, continue with SO 4.5.1. If not, defer the problem according to action SO 4.4.10. An estimate of the resources and skills required for solution investigation and resolution are determined. This includes the number of required personnel days, duration, and additional costs. Verify whether the workaround available modifies the priority or planning for resolving the problem. If an effective workaround is found, the target dates to resolve the known error can be modified. If a workaround is not found, the priority of the known error can be raised. Update the planning and milestones for the solution investigation and resolution deadline. If required, the planning is discussed and reviewed with stakeholders. If the known error is not resolved, a decision must be made to continue with defining other solution candidates, or to defer the problem.	Problem Manager
SO 4.4.10	Defer problem and explain reasons	The problem and known error are deferred for a specified period of time by assigning a low priority. After the specified period of time, the problem is reviewed to determine next steps.	Problem Manager

Known Error Investigation (process SO 4.5)

The Known Error Investigation process is aimed at defining a temporary fix or permanent solution for the known error. Different solution alternatives can be evaluated until a definitive solution can be proposed to the Problem Manager.

Different resources and skills can be assigned during this stage to ensure that a solution or workaround can be defined within the specified time frame.

Details for this process can be seen in the following figure and table.

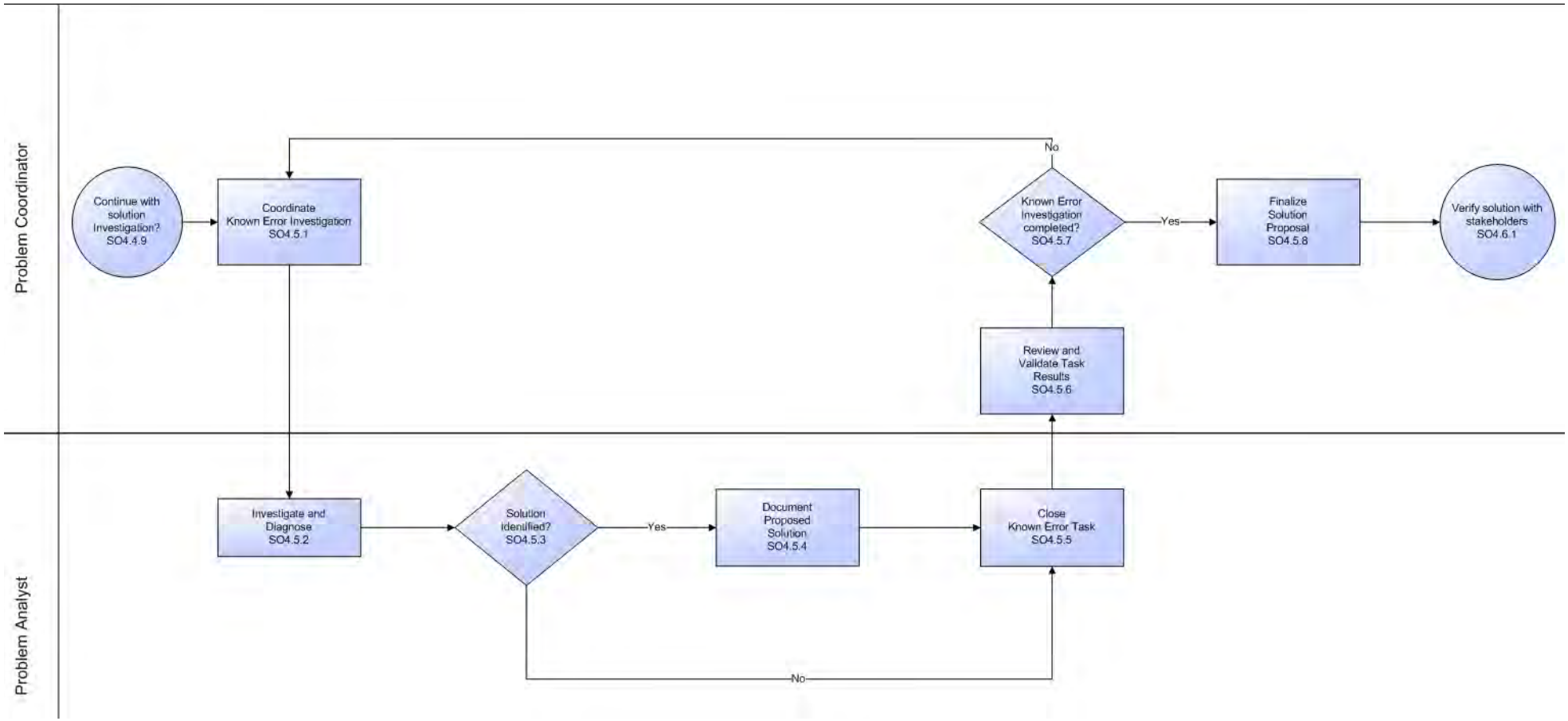

Figure 9-5 Known Error Investigation workflow

Table 9-5 Known Error Investigation process

Process ID	Procedure or Decision	Description	Role
SO 4.5.1	Coordinate Known Error Investigation	The Problem Coordinator assigns one or more known error tasks to Problem Analysts to investigate and determine appropriate solutions or fixes for the known error.	Problem Coordinator
SO 4.5.2	Investigate and diagnose	• Determine solution for the error. • Determine possible workarounds or temporary fixes for the known error. • Depending on the priority and impact of the known error, focus on defining a temporary fix that can be proposed or implemented within a short time frame. Workarounds serve as a temporary alternative to provide restoration to the affected service, or as a temporary service improvement in cases where a permanent fix is not yet available or feasible. Determine solution candidates to resolve the known error. If the temporary fix must be implemented through a change, consider the fix as a solution candidate. The Problem Analyst determines whether he or she is able to resolve the error, or if additional resources are required (that is, skills and time).	Problem Analyst
SO 4.5.3	Solution identified?	If a solution candidate is found, continue with SO 4.5.4. If not, continue with SO 4.5.5.	Problem Analyst
SO 4.5.4	Document proposed solution	Finalize the solution documentation in the known error task. Make sure to include necessary actions to implement the solution. Continue with SO 4.5.5.	Problem Analyst
SO 4.5.5	Close known error task	After completion, the Problem Analyst closes the task. The closure code marks the task as completed successfully, or not. The Problem Coordinator is notified of this event.	Problem Analyst
SO 4.5.6	Review and validate task results	Review the proposed solution, as identified by the Problem Analyst. The solution is defined in the task. Update the known error with the updates from the task. Determine whether the proposed solution is acceptable (for example, by testing or discussing with other technical specialists). If multiple solutions are defined, select the best solution. Make sure that the validation process includes the following considerations: • Costs and resources needed to implement the solution • Risks to implement the solution	Problem Coordinator
SO 4.5.7	Known Error Investigation completed?	Determine whether the investigation is completed and if a solution is identified and documented. If a suitable solution is identified (including cost and resource constraints), continue with SO 4.5.8, and then SO 4.6.1 If not, continue with SO 4.5.1. If a solution is successfully determined and if no workaround has yet been found, the Problem Coordinator (together with the Problem Manager) must assess whether there is still a need to find a workaround. If a permanent resolution can be implemented quickly, there may be no need to continue working on defining workarounds. If planning and implementing a permanent fix will take time or is too expensive, then work to identify an effective workaround should continue.	Problem Coordinator
SO 4.5.8	Finalize solution proposed	Document the solution, including an impact assessment, an estimation of the costs, and resources required, to implement the solution.	Problem Coordinator

Known Error Solution Acceptance (process SO 4.6)

The Known Error Solution Acceptance process begins when a solution has been identified and documented. This process reviews and approves the solution for implementation, taking into consideration the cost and impact of the solution with stakeholders.

When the root cause has been identified and a decision to resolve it has been made, the resolution should be advanced via the Change Management process, with a service request, or assigned to a Problem Coordinator so that a Problem Analyst can directly apply the fix.

Depending on the fix, the resolution can be applied through the following methods:

- Change that follows the Change Management process by creating a request for change.
- Standard request, which can be ordered through the service request from the catalog. For example, this might include a hardware replacement or installation of software.
- Resolutions that are applied directly. For example, this might include operations procedures and daily maintenance activities.

Information on a workaround, permanent fixes, or progress of problems should be communicated to those affected or required in order to support affected services. In the case where a solution is not correct or not acceptable, the Problem Manager determines whether to continue to investigate the solution, or defer the known error and problem.

Details for this process can be seen in the following figure and table.

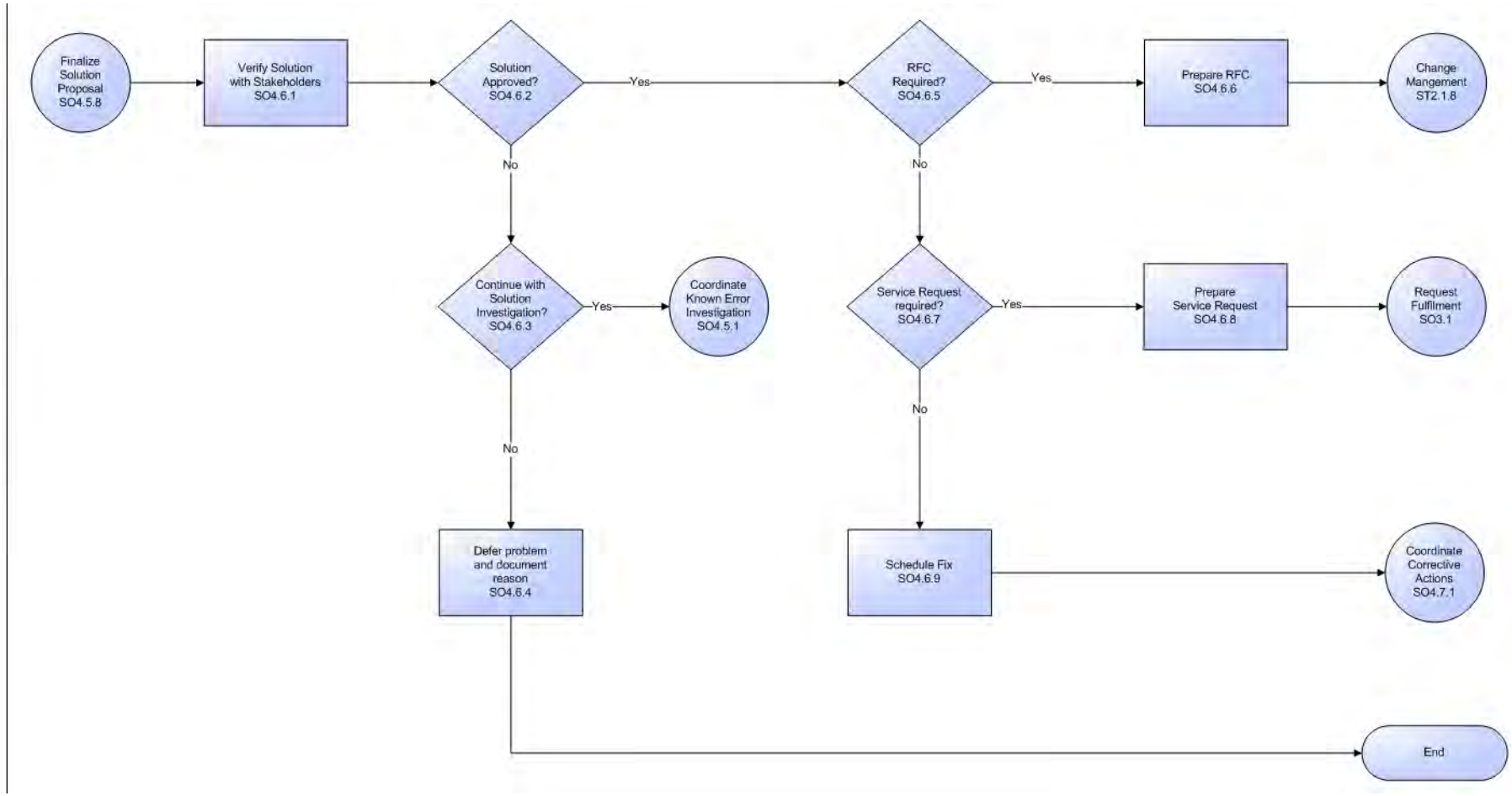

Figure 9-6 Known Error Solution Acceptance workflow

Table 9-6 Known Error Solution Acceptance process

Process ID	Procedure or Decision	Description	Role
SO 4.6.1	Verify solution with stakeholders	Review and validate the proposed solution. Discuss the cost and impact of the solution with stakeholders during a Problem Management meeting.	Problem Manager
SO 4.6.2	Solution approved?	If the solution is approved, go to SO 4.6.5. If not, continue with SO 4.6.3.	Problem Manager
SO 4.6.3	Continue with solution investigation?	Determine whether to continue with the solution investigation phase or defer the problem if no effective fix can be provided (for example, due to financial and resource constraints). If you want to continue with the solution investigation phase, go to SO.4.5.1. If not, go to SO 4.6.4.	Problem Manager
SO 4.6.4	Defer problem and document reason	The known error and related problem will be deferred for a specified period of time. Update the status (deferred), priority, and schedule of the problem and known error. Determine a date by which the problem and known error must be reviewed for additional actions.	Problem Manager
SO 4.6.5	RFC required?	Determine whether the solution must be implemented through a formal change procedure. If yes, go to SO 4.6.6. If not, continue with SO 4.6.7.	Problem Manager
SO 4.6.6	Prepare Request for Change (RFC)	Prepare for the RFC by collecting details required for completion of the RFC. Follow the procedures, as defined by Change Management, to create the RFC.	Problem Manager
SO 4.6.7	Service request required?	Determine whether the solution must be implemented through a standard request fulfillment procedure. If yes, go to SO 4.6.8. If not, continue with SO 4.6.9.	Problem Manager
SO 4.6.8	Prepare service request	Prepare for the service request by collecting details required for completion of the request. Follow the procedures, as defined by request fulfillment, to create the service request.	Problem Manager
SO 4.6.9	Schedule fix	Schedule the implementation of corrective actions to resolve the known error. Assign the known error to the appropriate Problem Coordinator, and then continue with SO 4.7.1.	Problem Manager

Known Error Resolution (process SO 4.7)

Known Error Resolution is the process by which stakeholders can ensure that a fix for a known error is implemented. This occurs after a solution for the known error has already been determined by the Problem Analyst, validated by the Problem Coordinator, and approved by the Problem Manager. The determination has been made that the fix can be applied through a change request, service request, or directly by the Problem Analyst.

If a Known Error Resolution is going to be implemented using a change request or service request, the actual deployment is executed by that Service Manager application.Throughout the resolution process, Problem Management should obtain regular reports from Change Management on progress in resolving problems and errors.

A known error should only be closed when a corrective change has been successfully applied, or if the error is no longer applicable (for example, due to a service no longer in use). The steps in the Known Error Resolution process are performed by the following roles:

- Problem Coordinator
- Problem Analyst
- Change Coordinator

Details for this process can be seen in the following figure and table.

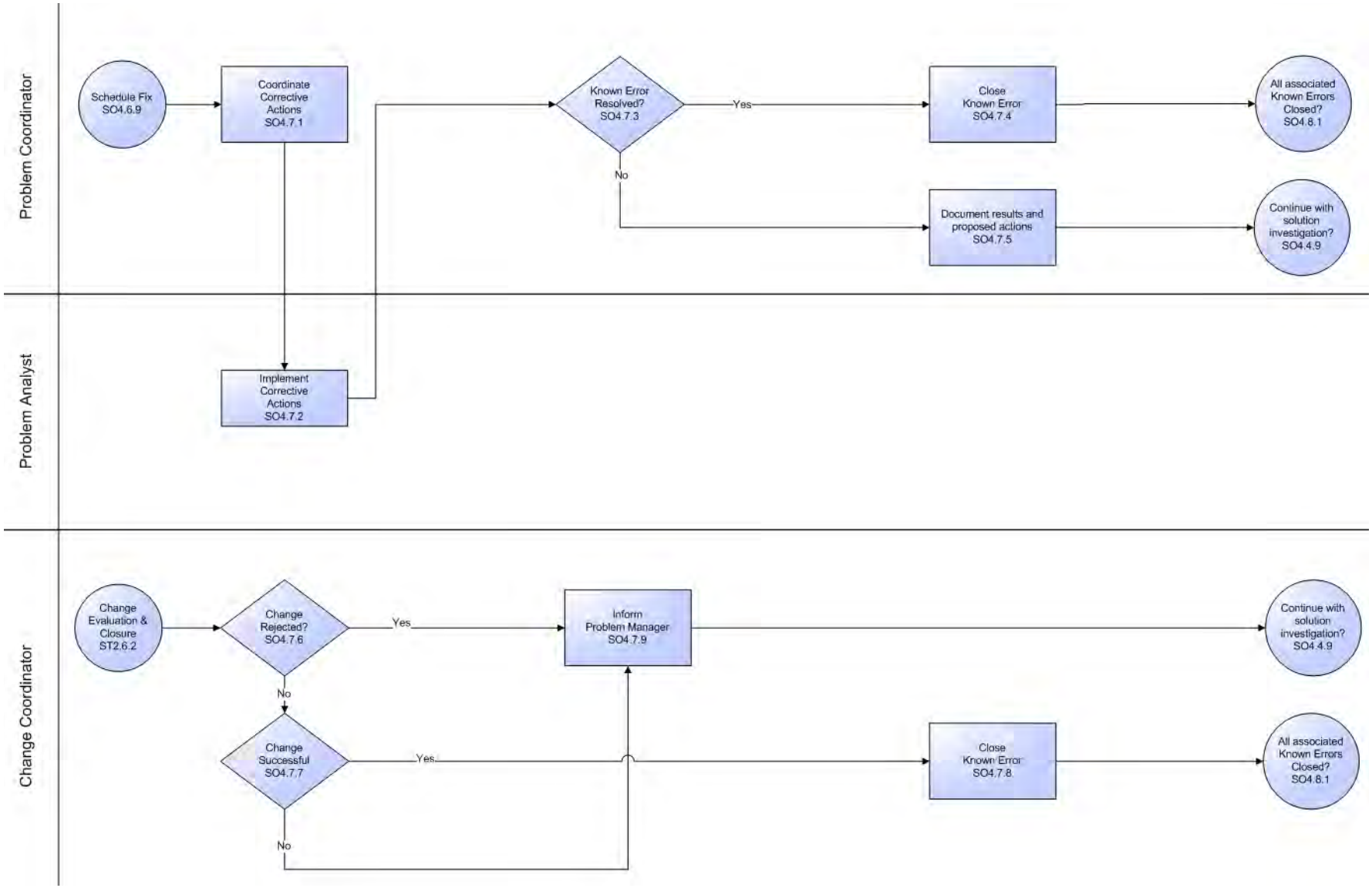

Figure 9-7 Known Error Resolution workflow

Table 9-7 Known Error Resolution process

Process ID	Procedure or Decision	Description	Role
SO 4.7.1	Coordinate corrective actions	Assign tasks to Problem Analysts to execute the resolution tasks to resolve the known error.	Problem Coordinator
SO 4.7.2	Implement corrective actions	The Problem Analyst implements the solution or fix to remove the known error and thus prevent any recurrence of incidents. After completion, the task is closed and the Problem Coordinator is informed.	Problem Analyst
SO 4.7.3	Known error resolved?	Ensure that the known error is resolved. If yes, continue with SO 4.7.4. If not, go SO 4.7.5.	Problem Coordinator
SO 4.7.4	Close known error	Update the known error record (document actions taken), and then close the known error. Continue with SO 4.8.1.	Problem Coordinator
SO 4.7.5	Document results and proposed actions	This action is triggered if the applied fix did not resolve the error. Document test results and determine appropriate actions. Inform the Problem Manager to determine next steps. Continue with SO 4.4.9.	Problem Coordinator
SO 4.7.6	Change rejected?	If the change is rejected, go to SO 4.7.9. If not, go to SO 4.7.7.	Change Coordinator
SO 4.7.7	Change successful?	If the change is successful (as verified by the change process), the known error can be closed (SO 4.7.8). If not, continue with SO 4.7.9.	Change Coordinator
SO 4.7.8	Close known error	After the known error is resolved, the record is closed. Continue with SO 4.8.1 in the problem closure process.	Change Coordinator
SO 4.7.9	Inform Problem Manager (and Problem Coordinator)	The Problem Manager is notified that the resolution has failed. Continue with SO 4.4.9 to determine next steps and appropriate actions.	Change Coordinator

Problem Closure and Review (process SO 4.8)

After a known error has been resolved, any related problem(s) are automatically forwarded from the Problem Resolution phase to the Problem Closure and Review phase. In this phase, the problem(s) must be reviewed to determine whether all related errors have been resolved and to validate that the problem is resolved as well.

A process must be in place to close problem tickets, either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.

A problem review should be scheduled whenever an investigation into unresolved, unusual, or high-impact problems justifies it. The purpose of the problem review is to seek improvements to the process and to prevent recurrence of incidents or mistakes.

Problem reviews typically include the following elements:

- Reviews of individual incident levels and problem status against service levels.
- Management reviews to highlight those problems that require immediate action.
- Management reviews to determine and analyze trends, and to provide input for other processes, such as user education and training.

Problem reviews should include identifying the following elements:

- Trends (for example, recurring problems, recurring incidents, and known errors).
- Recurring problems of a particular classification component or location.
- Deficiencies caused by lack of resources, training, or documentation.
- Non-conformances (for example, against standards, policies, and legislation).
- Known errors in planned releases.
- Staff resource commitment in resolving incidents and problems.
- Recurrence of resolved incidents or problems.

Improvements to the service or the Problem Management process should be recorded and fed into a service improvement plan. The information should be added to the Problem Management knowledgebase. All relevant documentation should be updated (for example, user guides and system documentation).

Details for this process can be seen in the following figure and table.

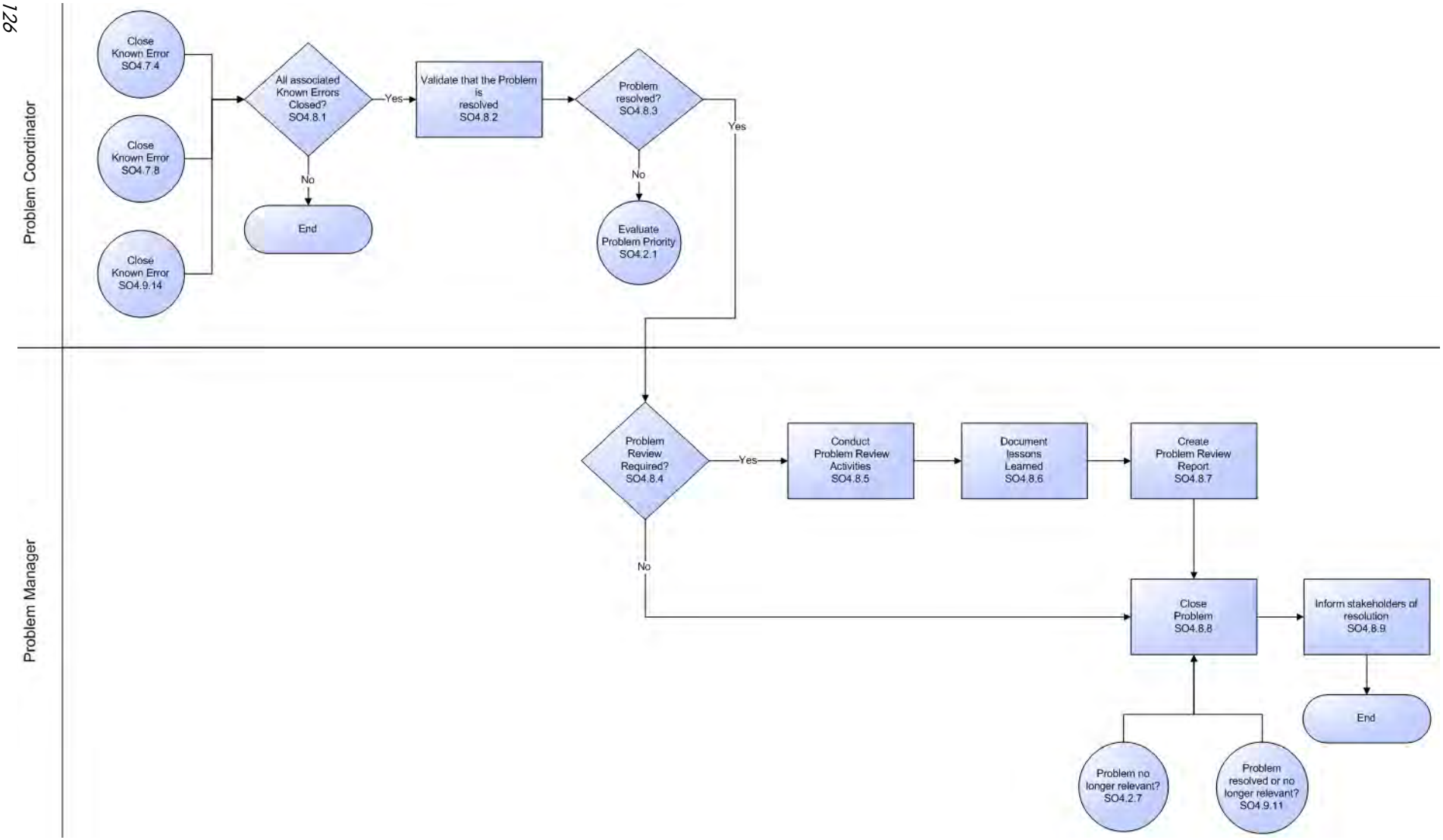

Figure 9-8 Problem Closure and Review workflow

Table 9-8 Problem Closure and Review process

Process ID	Procedure or Decision	Description	Role
SO 4.8.1	All associated known errors closed?	Check whether all related known errors are closed or resolved. If all known errors are closed, update the Problem Management phase to Problem Closure and Review, and then continue with SO 4.8.2. If all known errors are not closed, the process ends.	Problem Coordinator
SO 4.8.2	Validate that the problem is resolved	Validate whether the problem is resolved and continue with SO 4.8.3. Depending on the nature of the problem, you may be required to keep the problem open for a specified period of time (for example, for an evaluation period). If no incidents reoccur, the problem can be closed.	Problem Coordinator
SO 4.8.3	Problem resolved?	If the problem is resolved, continue with SO 4.8.4. If not, continue with SO 4.2.1. In some cases, it becomes apparent that another error prevents the complete resolution of the problem (for example, when the problem is caused by multiple errors). In this case a new known error may have to be investigated.	Problem Coordinator
SO 4.8.4	Review required?	Determine whether a formal problem review is appropriate. If yes, continue with SO 4.8.5. If not, continue to SO 4.8.8.	Problem Manager
SO 4.8.5	Conduct problem review activities	Initiate problem review activities and coordinate the formal review process. Include all parties involved in the Problem Resolution.	Problem Manager
SO 4.8.6	Document lessons learned	Document the problem review results and lessons learned.	Problem Manager
SO 4.8.7	Create problem review report	Create a formal problem review report and inform the stakeholders.	Problem Manager
SO 4.8.8	Close problem	Update the problem ticket prior to closing the record. Ensure all information about the problem is complete and select a closure code.	Problem Manager
SO 4.8.9	Inform stakeholders of resolution	Inform stakeholders that the problem is resolved.	Problem Manager

Problem and Known Error Monitoring (process SO 4.9)

Problem Management monitors the continuing impact of problems and known errors on user services. In the Problem and Known Error Monitoring process, the Problem Manager periodically reviews the problem and known error records, and monitors the progress of activities in those records against the target dates agreed to with stakeholders.

HP Service Manager tracks individual problems and their associated known error activities. The Problem Manager evaluates the progress of those activities against the plans and associated budget. In the event that an impact becomes severe, the Problem Manager escalates the problem. In some cases, the Problem Manager refers the escalated problem to an appropriate board to increase the priority of the request for change or to implement an urgent change, as needed.

The Problem Manager monitors the progress of each Problem Resolution against service level agreements, and periodically informs the stakeholders of that progress.

Details for this process can be seen in the following figure and table.

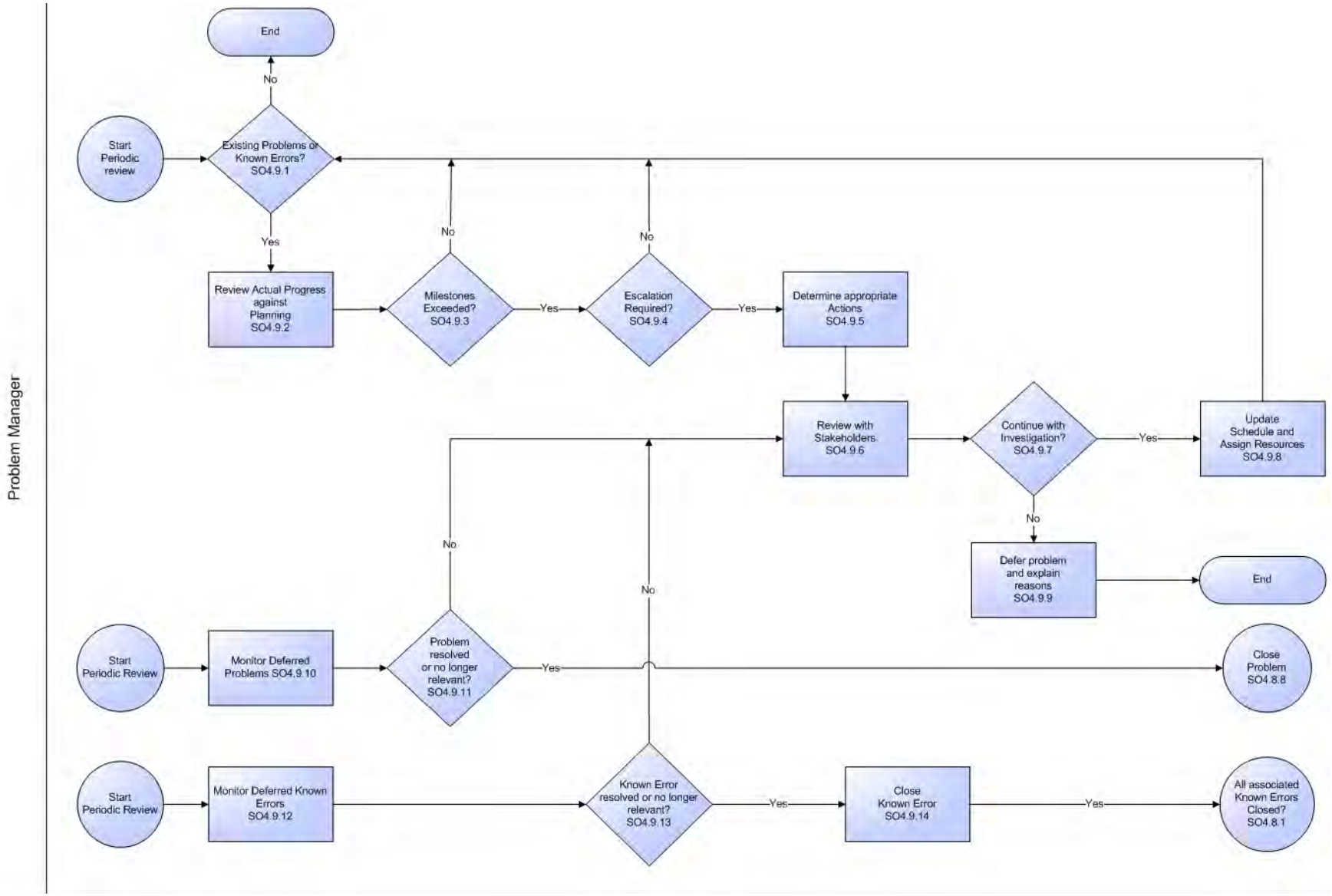

Figure 9-9 Problem and Known Error Monitoring workflow

Table 9-9 Problem and Known Error Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 4.9.1	Existing problems or known errors?	Periodically the problem and known error records are reviewed to evaluate the progress against the planning (and associated budget). The Problem Manager creates a list (or report) of all active problems and known errors. If there are any outstanding problems or known errors, go to SO 4.9.2. If not, then no further action is required.	Problem Manager
SO 4.9.2	Review actual progress against planning	The progress of the problem and known error activities is reviewed against the target dates, as communicated or agreed with stakeholders.	Problem Manager
SO 4.9.3	Milestone exceeded?	Check whether a milestone has been (or is expected to be) exceeded. If so, go to SO 4.9.4. If not, continue with the next problem or known error in the list (SO 4.9.1).	Problem Manager
SO 4.9.4	Escalation required?	Check whether escalation is required. If not, continue with next problem or known error in the list (SO 4.9.1). If required, contact the Problem Coordinator or Problem Analyst for additional information (for example, estimate to complete time), and go to SO 4.9.5.	Problem Manager
SO 4.9.5	Determine appropriate actions	The Problem Manager investigates the cause of delay and determines corrective actions (for example, assign additional resources or modify planning).	Problem Manager
SO 4.9.6	Review with stakeholders	Adjustments to the planning and actions are discussed with stakeholders. The progress is discussed with stakeholders to determine priorities and alternative plans.	Problem Manager
SO 4.9.7	Continue with investigation?	Determine whether to continue to spend resources on investigation or resolution of the problem. If required, additional resources are assigned (see SO 4.9.8). If continuation of the investigation is not feasible, the problem can be deferred (see SO 4.9.9).	Problem Manager
SO 4.9.8	Update schedule and assign resources	Update the planning and resources assigned to the problem or known error, and then continue with the next problem or known error in the list (SO 4.9.1).	Problem Manager
SO 4.9.9	Defer problem and explain reasons	The problem and known error will be deferred for a specified period of time (low priority). After the specified period of time, the problem is reviewed to determine next actions. End of process.	Problem Manager
SO 4.9.10	Monitor deferred problems	Periodically review the deferred problems to determine whether additional actions are required. The Problem Manager creates a list (or report) of all deferred problems.	Problem Manager
SO 4.9.11	Problem resolved or no longer relevant?	If the problem is resolved or no longer relevant, the problem can be closed. Continue with SO 4.8.8 to close the problem. If not, go to SO 4.9.6 to determine next steps.	Problem Manager

Table 9-9 Problem and Known Error Monitoring process (cont'd)

Process ID	Procedure or Decision	Description	Role
SO 4.9.12	Monitor deferred known errors	The Problem Manager periodically reviews the deferred errors to determine whether circumstances have changed that require continuing with the investigation and resolution. The Problem Manager creates a list (or report) of all deferred known errors.	Problem Manager
SO 4.9.13	Known error resolved or no longer relevant?	Determine whether the known error is resolved (for example, due to an upgrade or change) and whether the error is no longer relevant for the business. If the error is resolved, continue with SO 4.9.14 to close the known error. If not, continue with SO 4.9.6 to determine next steps.	Problem Manager
SO 4.9.14	Close known error	Continue with SO 4.8.1 to close the known error.	Problem Manager

10 Problem Management Details

HP Service Manager uses the Problem Management application to enable the Problem Management process. The main function of Problem Management is to identify and resolve problems and known errors.

In Problem Management, the Problem Manager plans and prioritizes problems. The Problem Coordinator manages root cause analysis and resolution, and the Problem Analyst diagnoses the root cause of the problem and proposes and implements solutions for them.

This section describes selected Problem Management fields in the out-of-box Service Manager system.

Topics in this section include:

Problem form after escalation from incident

After the incident is escalated, the problem ticket enters the Problem Detection, Logging and Categorization phase.

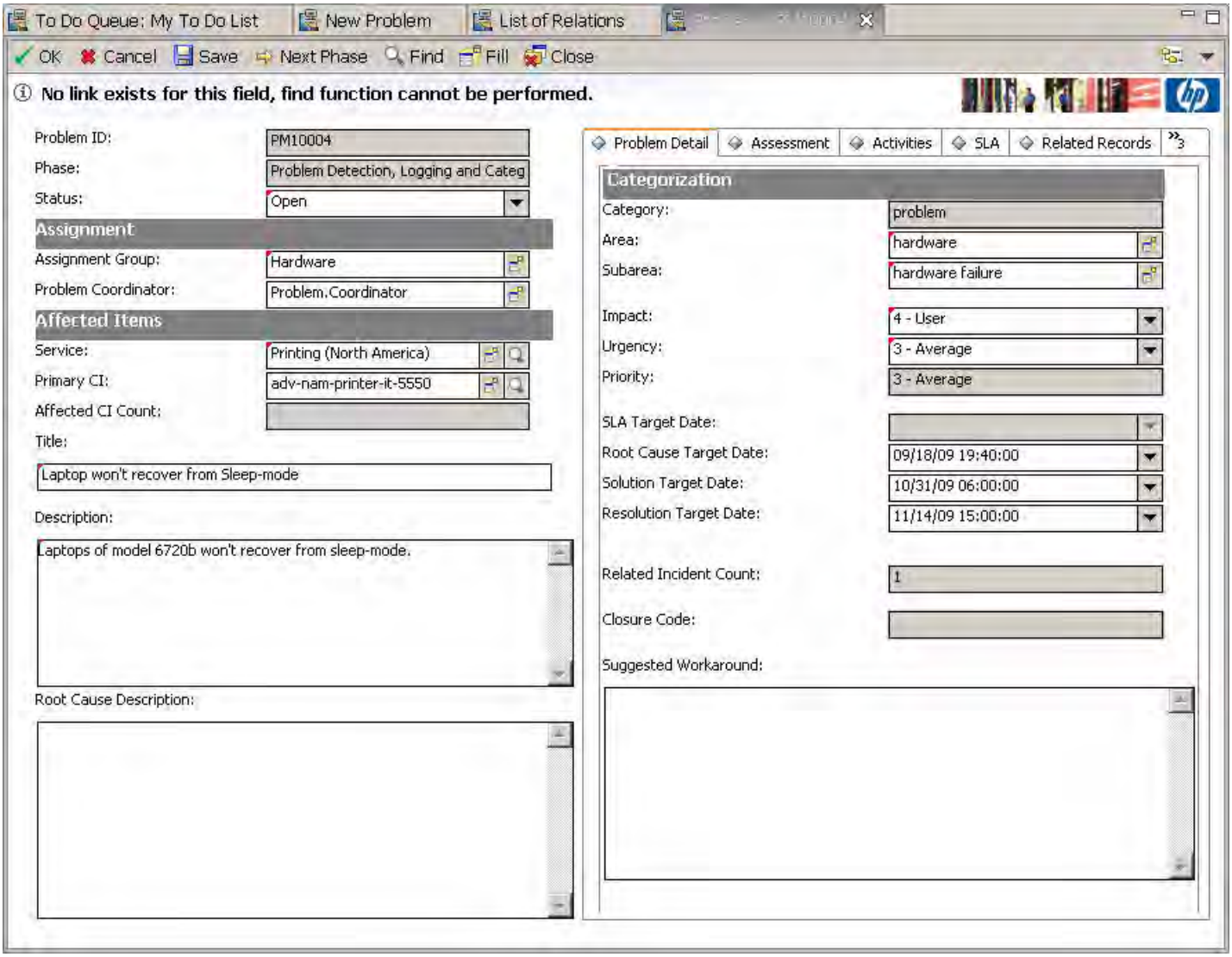

Figure 10-1 New problem form

Problem Control form details

The following table identifies and describes some of the features on the Problem Control forms.

Table 10-1 Problem Management form details

Label	Description
Problem ID	Specifies the unique ID of the associated problem ticket. This is a system-generated field.
Phase	This is a system-generated field. These phases are available out-of-box: • Problem Detection, Logging, and Categorization • Problem Prioritization and Planning • Problem Investigation and Diagnosis • Problem Resolution • Problem Closure and Review
Status	Specifies the status of the problem. This field is not affected by the phase of the problem. The Problem Phase does not automatically change the status except when you first open a problem. All other status changes must be done manually. There are several reasons to change the status of a problem ticket, for example, when you are waiting for a vendor's information. These status are available out-of-box: • Open — The problem has been opened, but it is not currently being worked on. • Accepted — The Problem Coordinator has accepted this record as his or her responsibility. • Work in Progress — The problem is being addressed. • Pending Vendor — The Problem Coordinator contacted the vendor and the vendor has to provide info or send a part. • Pending User — Problem Coordinator contacted the user and needs more information from him the user. • Rejected — The Problem Coordinator has rejected responsibility for this record. • Deferred — Because of several possible constraints, must postpone fixing problem until later release. (This may happen in prioritization and planning, but it can also happen later in the process.) This is a required field.

Table 10-1 Problem Management form details (cont'd)

Label	Description
Assignment > Assignment Group	The group assigned to work on the problem. For a description of this field see the Assignment Group field description in (Incident Management form details on page 86) as this field functions similarly. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. Tip: You may want to change the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager This is a required field.
Assignment > Problem Coordinator	The name of the person assigned to coordinate the work on this problem. If the Assignment Group is filled in, the system will populate this field with the pre-defined Problem Coordinator for that group. This person can be changed to any other member of that group using the Fill function. The operator you select should be a member of the assignment group and should have the user role of Problem Coordinator to be assigned Problem Coordinator.
Affected Items > Services	Specifies the Service affected by the problem. This field is populated with data from the related incident when a problem is created from an incident. For additional field description information, see User Interaction Management form details on page 44. This is a required field.
Affected Items > Primary CI	Specifies the name of the failing Configuration Item (CI). The Primary CI identifies the CI that causes the service to go down or be unavailable. The affected CIs in the related incidents and interactions are all of the CIs affected by the service. It is the primary CI that must be fixed to restore the service. For example, if a mail service goes down because of a disk error on the server, the mail server that is the primary CI. Every CI connecting to the mail service (has Outlook installed) is an affected CI.
Affected Items > Affected CI Count	A system-generated count of the number of CIs affected by the outage. The count does not include the Primary CI. Affected CI count is based on the number of items entered in the Assessment notebook tab. It is calculated based on what is in the Assessment notebook tab in the Affected CIs table.
Title	A short description summarizing the problem. This field is prepopulated with data from an incident when a user opens a problem from an incident. This is a required field.

Table 10-1 Problem Management form details (cont'd)

Label	Description
Description	A detailed description of the problem. This field is prepopulated with data from the incident when a user creates a problem from an incident. This is a required field.
Root Cause Description	A detailed description of what caused the problem. You can not move on from the Problem Investigation and Diagnosis phase until you have filled in this description. That phase is not complete until the cause of the problem is known.
Problem Detail > Category	This field is prepopulated with the value "problem". The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44 and Interaction categories on page 50.
Problem Detail > Area	This field is prepopulated with data from an escalated incident. Service Manager displays different lists of areas, depending on the category you selected. For more information on categories, and the areas and subareas associated with them, see Interaction categories on page 50. The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44.
Problem Detail > Sub-area	The third level of classification, mainly used for reporting purposes. This field is prepopulated with data from an escalated incident. Service Manager displays different lists of subareas, depending on the area selected. For more information on categories and the areas and subareas associated with them, see Interaction categories on page 50. The out-of-box data is the same as in Interaction Management. For additional information, see User Interaction Management form details on page 44.
Problem Detail > Impact	This field is prepopulated with data from an incident. It specifies the impact the problem has on the business. The impact and the urgency are used to calculate the priority. These impacts are available out-of-box: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User The out-of-box data is the same as Interaction Management and Incident Management.
Problem Detail > Urgency	This field is prepopulated with data from the incident. The urgency indicates how pressing the problem is for the organization. The urgency and the impact are used to calculate the priority. For additional information, see User Interaction Management form details on page 44.
Problem Detail > Priority	The order in which to address this problem in comparison to others. A priority value calculated using initial impact and urgency. This field only appears for problems being updated or escalated from incidents.
Problem Detail > SLA Target Date	This is a system-generated field that displays the date and time of when the next SLO will occur. The SLA Target date is the date when the system generates the alerts because the SLA is breached. For additional information see Incident Management form details on page 86.

Table 10-1 Problem Management form details (cont'd)

Label	Description
Problem Detail > Root Cause Target Date (Root Cause Identified Date)	The field specifies the expected date to find the root cause of the problem. The field label (name) changes to Root Cause Identified Date during the Problem Investigation and Diagnosis phase. You should base the date on the target and identified dates on the SLA. Once the root cause is found, this field becomes the identified date. This field become required during the Prioritization and Planning phase to assist prioritization and planning in Problem Management processing. This is a required field.
Problem Detail > Solution Target Date (Solution Identification Date)	The field label (name) changes to Solution Identification Date during the Problem Investigation and Diagnosis phase. The Solution Target date is when you identify the solution. It also becomes required during this phase. This is a required field.
Problem Detail > Resolution Target Date (Problem Resolution Date)	The Problem Resolution date should be approximately the same as the SLA Target date. The Problem Resolution date is the date when you plan to click the Close button for the record. It should be before the SLA Target date. It has the Problem Management past due alert attached to it. The field label (name) changes to Problem Resolution Date during the Problem Investigation and Diagnosis phase. This field is required during Prioritization and Planning phase. This is a required field.
Problem Detail > Related Incident Count	This is a system-generated field. The related incident count is the number of incidents related to problem, as recorded in the scrlation table. To relate an incident to a problem, a user clicks Related > Problems > Associated. This is what populates this field with data.
Problem Detail > Closure Code	Uses a pre-defined closure code to specify the way the problem has been solved. This field is enabled and required during Problem Closure and Review phase. The out-of-box data is the same as that for incidents and interactions. For more information, see User Interaction Management form details on page 44. This is a required field.
Problem Detail > Suggested Workaround	Describes a temporary solution or workaround. This field needs to be filled before a known error can be created.
Assessment > Estimated # of Mandays	Specifies a resource estimate to diagnose and resolve the problem. This data does not drive any action and is not required.
Assessment > Estimated Costs	Provides a resource (cost) estimate to diagnose and resolve the problem. This data does not drive any action and is not required.
Assessment > Affected CI's table	The affected Configuration Items (CIs) are CIs that will have an issue when the primary CI goes down. These field need to be filled in manually and are for information only. This data does not drive any action and is not required. The data displayed includes the following information: • Configuration Item • Device Type • Assignment Group

Table 10-1 Problem Management form details (cont'd)

Label	Description
Task > Task ID	This notebook tab is only enabled for the Problem Investigation and Diagnosis phase. Tasks can only be opened once the planning is complete. Every task has to be finished before the problem moves to the next phase. Use the Options menu and click Create a task to add a task to this tab. There is a wizard to assist you. The Task ID is system-generated. The Assignee is a person who is part of the assignment group that is defined for the CI. For example, if tasks are assigned to the hardware assignment group, then a person within the group can be assigned to the task
Submit button	This button creates (or opens) the problem ticket after all of the required fields are complete.
Next Phase button	This button is used to end one phase and proceed to the next phase after all of the required fields are complete
Prior Phase button	This button is used change the problem from the current phase to the previous phase. You should use this button if something went wrong in your process. For example, when you are in the Problem Investigation and Diagnosis phase, and it turns out that you made mistake in the Problem Prioritization and Planning phase, you have to go back to that phase and begin planning again.
Options > Open Known Error button	This button is only available from Problem Investigation and Diagnosis phase or later. The best practice is to create known error at later phases than the Problem Investigation and Diagnosis phase.
Options > Create Tasks button	This button creates or opens a task for the problem. This button is only available from the Problem Investigation and Diagnosis phase or later.
Close button	This button closes the problem ticket.

Problem Management form after escalation to known error

Once a workaround has been found, the problem is escalated to a known error.

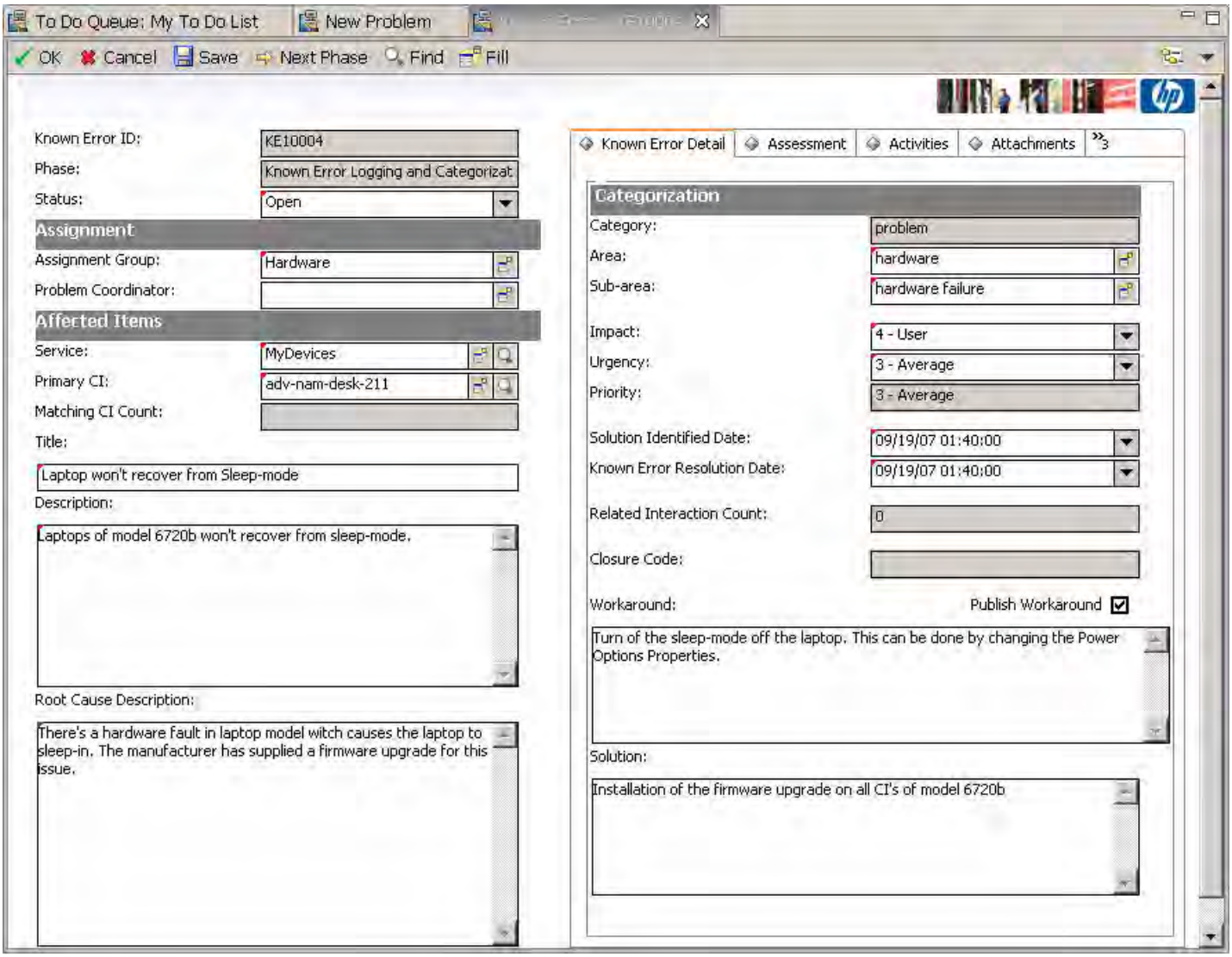

Figure 10-2 New known error form

Error Control form details

The following table identifies and describes some of the features on the known error forms.

Table 10-2 Field descriptions for known error forms

Label	Description
Known Error ID	This is a system-generated field.
Phase	This is a system-generated field. These phases are available out-of-box: • Known Error Logging and Categorization • Known Error Investigation • Known Error Solution Acceptance • Known Error Resolution
Status	This is a system-generated field. The out-of-box data is the same status data as that of an incident or interaction except that a known error cannot have a status of inactive. The known error process does not automatically change the status of the record. The status can be set independently of the phase and within one phase the status can be set to any of the statuses available because status and phase are independent of each other in the known error process. These statuses are available out-of-box: • Open • Accepted • Work in Progress • Pending Vendor • Pending User • Rejected • Deferred This is a required field.
Assignment > Assignment Group	The data in this field is inherited from the problem ticket and the field works as described in the Assignment Group field for a problem ticket. See page 134 for additional information.
Assignment > Problem Coordinator	This field is inherited from the problem ticket, and it specifies the person responsible for ensuring that this known error gets resolved. This field can be updated to change the person responsible for the known error.
Affected Items > Services	The data in this field is inherited from the problem ticket and the field works as described in the Services field for a problem ticket. See Table 10-1 on page 133 for additional information.
Affected Items > Primary CI	The data in this field is inherited from the problem ticket and the field works as described in the Services field for a problem ticket. See Table 10-1 on page 133 for additional information.
Affected Items > Matching CI Count	A system-generated count of the number of related CIs affected by the outage. See Table 10-1 on page 133 for additional information.
Title	A brief description of the known error that is inherited from the problem ticket. This is a required field.

Table 10-2 Field descriptions for known error forms (cont'd)

Label	Description
Description	A detailed description of the known error that is inherited from the problem ticket. This is a required field.
Root Cause Description	The root cause description explains what caused the known error (problem) described in the description field. This field is inherited from the Root Cause Description in the problem ticket and is a required field because you cannot continue with the problem process without knowing the root cause of the problem. This is a required field.
Known Error Detail > Category	This is a system-generated field and for an out-of-box system the category is problem. The category defines the relevant process, and ensures that the correct process assumes control.
Known Error Detail > Area	This field is inherited from the problem ticket. It provides the same out-of-box data as the interaction record and can be updated. For additional information, see Table 4-1 on page 44. This is a required field.
Known Error Detail > Sub-area	This field is inherited from the problem ticket. It provides the same out-of-box data as the interaction record and can be updated. For additional information, see Table 4-1 on page 44. This is a required field.
Known Error Detail > Impact	This field is inherited from the problem ticket. It provides the same out-of-box data as the interaction record and can be updated. For additional information, see Table 4-1 on page 44. This is a required field.
Known Error Detail > Urgency	This field is inherited from the problem ticket. It provides the same out-of-box data as the interaction record and can be updated. For additional information, see Table 4-1 on page 44. This is a required field.
Known Error Detail > Priority	This is a system-generated field. For additional information, see Table 4-1 on page 44.
Known Error Detail > Solution Identified Date	This field is inherited from the problem ticket. Typically, the underlying cause has been identified when the known error is opened. The goal of this process is to identify the solution. This date indicates when the solution was found. For additional information, see Table 4-1 on page 44. This is a required field.
Known Error Detail > Known Error Resolution Date	The user specifies the date and time when the known error is expected to be resolved. It does not affect any of the other fields. This is a required field.
Known Error Detail > Related Interaction Count	This field shows how many interactions were closed directly using the workaround of this known error. Interactions can be closed during the escalation process, allowing association to an known error. The count therefore shows the success rate of the workaround.
Known Error Detail > Closure Code	Specifies a pre-defined closure for describing how the known error has been resolved. This field is enabled and required during the Known Error Resolution phase. The out-of-box data is the same as that for problem, incidents and interactions. For more information, see User Interaction Management form details on page 44. This is a required field.
Known Error Detail > Workaround	This field describes a workaround that enables users to get round the issue described in the problem ticket.

Table 10-2 Field descriptions for known error forms (cont'd)

Label	Description
Known Error Detail > Solution	This field should describe permanent solution for the known error. This field becomes required on completion of the Known Error Investigation phase.
Assessment > Estimated # of Mandays	Specifies a resource estimate to diagnose and resolve the known error. This data does not drive any action and is not required.
Assessment > Estimated Costs	Provides a resource (cost) estimate to diagnose and resolve the problem. This data does not drive any action and is not required.
Assessment > Matching	The matching Configuration Items (CIs) are CIs that will have an issue when the primary CI goes down. This field is inherited from the problem ticket. These field can be filled in manually and are for information only. This data does not drive any action and is not required. • Configuration Item List • Configuration Item • Device Type • Assignment Group
Task	This tab is only available when the record is in the Known Error Investigation phase. • Task ID • Status • Assignee • Configuration Item
Add	This button creates (or opens) the record after all of the required fields are complete.
Next Phase	This button is used to end one phase and proceed to the next phase after all of the required fields are complete
Prior Phase	This button is used change the known error from the current phase to the previous phase. You should use this button if something went wrong in your process.
Options > Create Tasks	This button is only available from the Known Error Investigation phase. Tasks can only be opened so that all investigation and planning is complete before solution is accepted. Every task has to be finished before the known error moves to the next phase.
Close	This button closes the known error record.

11 Change Management Overview

The HP Service Manager Change Management application, referred to as Change Management throughout this chapter, supports the Change Management process. It controls the process to request, manage, approve, and control changes that modify your organization infrastructure. This includes assets, such as network environments, facilities, telephony, and resources. Change Management enables you to control changes to baseline service assets and configuration items across the entire service life cycle.

This section describes how Change Management implements the best practice guidelines for the Change Management processes.

Topics in this section include:

Change Management within the ITIL framework

Change Management is addressed in ITIL's *Service Transition* publication. The document describes Change Management as the process responsible for ensuring that changes are recorded, evaluated, planned, tested, implemented, and reviewed in a controlled manner.

Change Management enables you to meet the following business objectives:

- Use standardized methods and procedures to ensure efficient and prompt handling of all changes.
- Record all changes to service assets and configuration items (CIs) in the Configuration Management System (CMS).
- Optimize overall business risk.
- Respond to customers' changing business requirements maximizes value and reduces incidents, disruptions, and rework.
- Respond to business and IT requests for changes aligns services with business needs.

The ITIL Change Management process model includes

- The steps to take to handle a change
- The order to take those steps in
- Who has responsibility for what part of the process
- Scheduling and planning
- When and how to escalate a change

Change Management application

The Change Management application supports the Change Management process by which the life cycle of changes is controlled. The primary objective of Change Management is to enable beneficial changes to be made with minimal disruption to IT Services. Changes are recorded, and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner. Change Management objectives are achieved by rigorous adherence to the process steps.

The Change Management application incorporates the essential concepts of ITIL to ensure that the best practices of IT service management are applied to Change Management to manage and control IT changes within the organization.

Differences between Change Management and Request Management

Change Management tracks changes to managed configuration items (CIs) in your infrastructure. Request Management only manages requests for products or services that do not change a managed attribute on a configuration item (CI). For example, a PC is typically a managed configuration item in most business infrastructures. However, the network password someone uses to log in to that PC is not typically a managed CI because it varies for each user.

- You use Change Management to track portions of the PC you want to standardize across your whole infrastructure such as the amount of hard drive space or the amount of RAM available.
- You use Request Management to manage products and services that affect the one person or group who uses the PC, such as a user's network password or desktop theme.

Change Management process overview

The Change Management process includes the activities necessary to control changes to service assets and configuration items across the entire service life cycle. It provides standard methods and procedures to use when implementing all changes.

The purpose of Change Management is to ensure that:

- Changes follow a set process.
- Appropriate users are notified at key points in the process.
- Progress of a change is monitored and notifications are issued if deadlines are missed.
- Changes are supported the change throughout a simple or complex life cycle.

Change categories and phases

Change Management uses categories to the classify the type of change requested. Out-of-box, each change type has its own category that defines the workflow and phases needed to satisfy the change request. They are described in detail in the following sections.

As a Service Manager administrator, you can use the default categories shipped with the product, or create new categories to match your business requirements.

- When you create a change request, you must select a category.
- Each category has predefined phases to ensure that the change occurs in an orderly progression. Phases are steps in the life cycle of the change or task. The phase determines which form is used with a record, along with behaviors such as approvals and edit.
- Each phase can optionally have one task, multiple tasks, or no tasks. A task is the work necessary to complete a single change phase.
- Each task also has its own category that is almost identical to the change category, but there are some differences. The task category can have multiple phases, but most often, just one.

A general overview of the Change Management processes and workflows is depicted in Figure 11-1,below. They are described in detail in Chapter 12, Change Management Workflows.

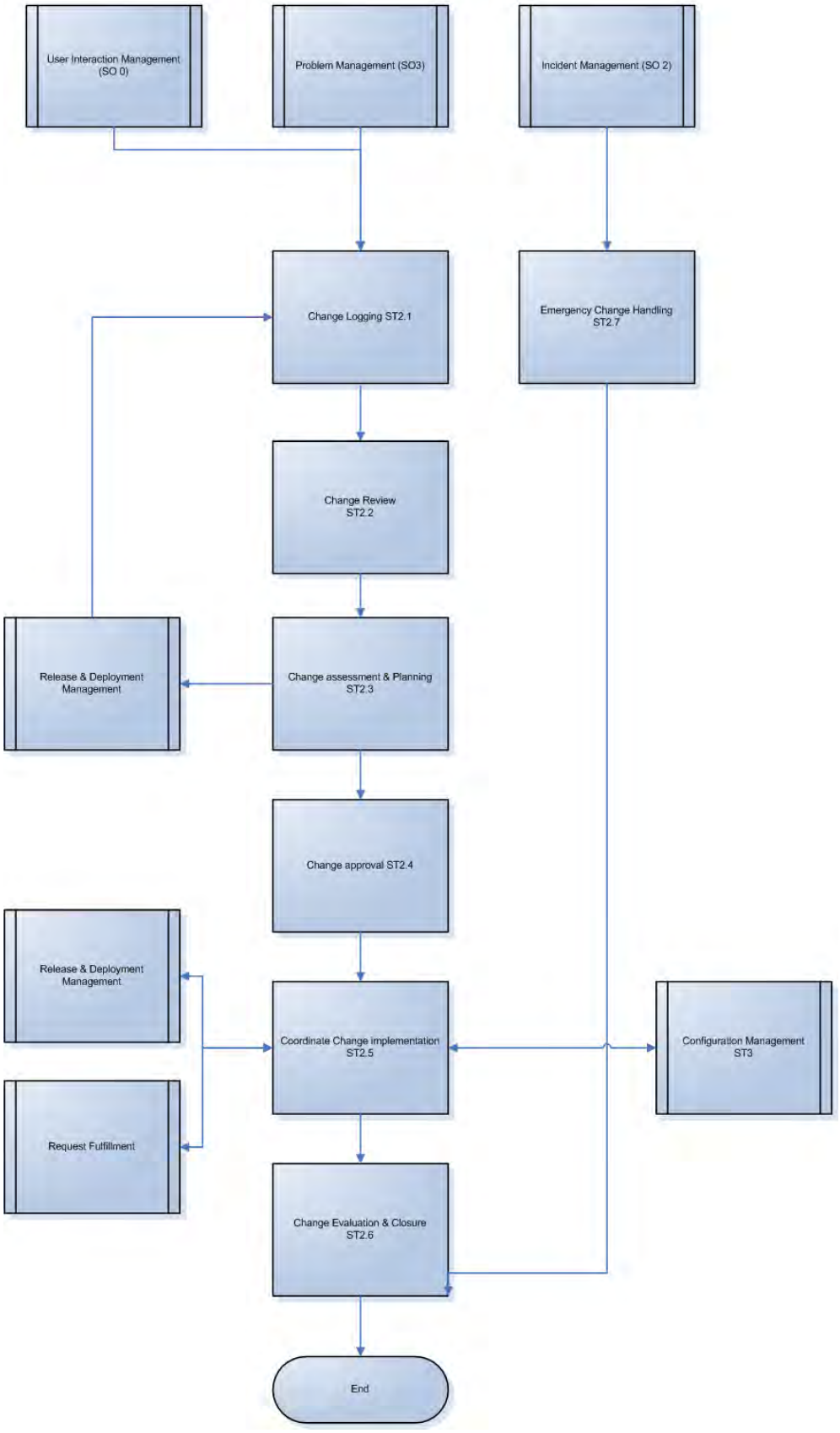

Figure 11-1 Change Management process diagram

Change Management categories

Service Manager categories classify and define the type of change requested. Each category has its own workflow process. The steps of the workflow are represented by the phases and tasks within the phase. Service Manager requires that every change have a change category and phase, but tasks are optional.

Service Manager provides ten out-of-box categories you can use to classify the changes in your business. Table 11-1 describes the out-of-box Change Management categories. Eight of these ten categories are available to regular users; the categories Default and Unplanned Change are assigned when changes are opened from other Service Manager applications.

Table 11-1 Change Management categories available out-of-box

Category	Description
CI Group	Manages Configuration Item Group changes.
Default	Category assigned when the change is created by escalation of a record from the Interaction, Incident, or Problem Management applications. See the Working with the default change category section that follows this table for more information.
Hardware	Manages hardware changes.
KM Document	Manages Knowledge Management documents.
Maintenance	Manages maintenance-related changes.
Network	Manages network-related changes.
Release Management	Manages the releases of hardware and software.
Software	Manages software-related changes.
Subscription	Manages changes to business service subscriptions.
Unplanned Change	Category associated with Service Manager integration with HP Universal CMDB (UCMDB). Indicates that an unscheduled change occurred. See the Working with the unplanned change category that follows this table for more information.

Working with the default change category

You should only use the Default change category when creating new changes that result from the escalation of other Service Manager activities, namely Interaction, Incident, or Problem Management. The default category is a temporary one, intended for Service Manager users such as Help Desk agents and Problem Managers who may not know or understand the Change process and its requirements.

The default change category intentionally does not use subcategories to further classify changes. This is done later, when a Change Manager reviews the change and reassigns it to the proper category. The Change Managers uses the information in the change and related records when categorizing the change. Never update a change that has been assigned to another category to use the default category.

Working with the unplanned change category

The category Unplanned Change is designed to be used as part of Service Manager's integration with the UCMDB. If UCMDB detects a change to a CI, one possible action is to open a change that is then categorized as an Unplanned Change since the change occurred without having been scheduled.

As part of the process, the manager decides if the change to the CI should be approved or not. If it is approved, the CI information in Service Manager is updated to match the change detected by UCMDB. If the change is rejected, a technician needs to change the CI back to its original state to match the CI information in Service Manager.

For more information about UCMDB, see HP Universal Configuration Management Database on page 191.

Change Management phases

Service Manager uses phases to describe the sequential steps needed to complete a change request. The phase also determines the forms users see, the approvals required to advance to the next phase, and the conditions that cause the system to issue alerts. Phases can only be completed in sequence. Use change tasks to complete actions in parallel.

For example, the following screen shows that the CI Group category consists of the following phases in sequence:

1. Designing a CI Group
2. Implementing a CI Group
3. Accept a CI Group

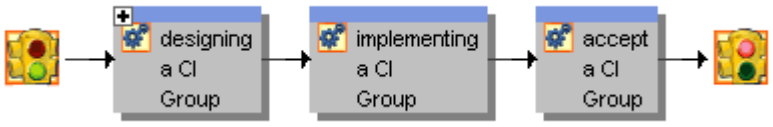

Figure 11-2 Sample phases of the CI Group category

Phases used in the out-of-box categories

Table 11-2 lists the phases that the out-of-box categories use to manage a change.

Table 11-2 Change Management phases for out-of-box categories

Category	Phases and workflow
CI Group	1. Change Logging > 2. Implementing a CI Group > 3. Accept a CI Group
Default	1. Change Logging > 2. Change Review (at this point the change should be reclassified into the appropriate category) > 3. Change Evaluation and Closure
Hardware	1. Change Logging > 2. Change Review > 3. Change Assessment and Planning > 4. Prepare for Change Approval > 5. Change Approval > 6. Change Implementation > 7. Change Evaluation and Closure
KM Document	1. Determine how to proceed with a Knowledge Document > 2. Revise a KM Document > 3. View a working copy document and add feedback > 4. Determine whether to Publish, Retire, or Revert a KM Document.
Maintenance	1. Change Logging > 2. Change Review > 3. Change Assessment and Planning > 4. Prepare for Change Approval > 5. Change Approval > 6. Change Implementation > 7. Change Evaluation and Closure
Network	1. Change Logging > 2. Change Review > 3. Change Assessment and Planning > 4. Prepare for Change Approval > 5. Change Approval > 6. Change Implementation > 7. Change Evaluation and Closure
Release Management	1. Assess Release > 2. Release plan and design> 3. Release build and test > 4. Release training (optional, depending on size of change) > 5. Release distribution > 6. Release back out (if verification fails) > 7. Release verification
Software	1. Change Logging > 2. Change Review > 3. Change Assessment and Planning > 4. Prepare for Change Approval > 5. Change Approval > 6. Change Implementation > 7. Change Evaluation and Closure
Subscription	1. Approve request for subscription or unsubscription > 2. Implement request for subscription or unsubscription > 3. Accept request for subscription or unsubscription
Unplanned Change	1. Discovery Assessment > 2. Discovery Back Out > 3. Discovery Implementation > 4. Discovery Verification

Phases for changes flagged as Emergency Changes

The Default, Hardware, Maintenance, Network, and Software categories allow an Emergency Change flag to be set. This flag adds Emergency Group Approval to the Change Approval phase. If a change is opened as an emergency, when the Change Logging phase is closed, it goes directly to the Prepare for Change Approval phase, skipping the Change Review and Change Assessment and Planning phases.

When a change is opened as an emergency, the Activities > Historic Activities tab shows the following description: “This change is logged as an Emergency Change.” If a change later becomes an emergency, the activity will say “This change has become an Emergency Change.” When the emergency flag is unchecked, the activity will say “This change has come back to the regular change process.” The Change Manager is also notified every time there is an activity (open, update, or closure of an emergency change).

Table 11-3 lists the phases for changes that have been flagged as Emergency Changes.

Table 11-3 Change Management phases emergency changes

Category	Phases and workflow
CI Group	1. Designing a CI Group > 2. Implementing a CI Group > 3. Accept a CI group
Default	1. Change Logging > 2. Change Review > 3. (At this point the category needs to be changed to one of the others listed in this table)
Hardware	1. Change Logging > 2. Prepare for Change Approval > 3. Change Approval > 4. Change Implementation > 5. Change Evaluation and Closure
Maintenance	1. Change Logging > 2. Prepare for Change Approval > 3. Change Approval > 4. Change Implementation > 5. Change Evaluation and Closure
Network	1. Change Logging > 2. Prepare for Change Approval > 3. Change Approval > 4. Change Implementation > 5. Change Evaluation and Closure
Software	1. Change Logging > 2. Prepare for Change Approval > 3. Change Approval > 4. Change Implementation > 5. Change Evaluation and Closure

Change Approvals

Each change phase may have one or more approvals. A change request cannot move to the next phase until all approvals associated with the current phase have been achieved. Adding an approval to a change phase allows a member of an approval group to review the business need behind the change request and approve or deny it. Typically only system administrators can add approvals to a change phase. Table 11-4 lists the change phases that require approvals out-of-box.

Table 11-4 Approvals for out-of-box phases

Change phase	Approvals required
Build and Test	Release Build and Test
CIGroupDesign	• CIGroupCAB • CIGroupAdmin • CIGroupTech
CIGroupImplement	CIGroup
Change Approval	• Approval • Emergency Group Approval
Discovery Assessment	Assessment
Distribution and Rollout	Release Distribution and Rollout
Plan and Design	Release Plan and Design
Subscription Approval	Subscription Approval
Verification	Release Verification

Approval definitions

Each approval requires an approval definition record. The approval definition record lists the operator or group who can approve or deny the change, the order in which the system requests approval, and the conditions under which the approver's review is required. For example, the picture below illustrates that the Assessment approval requires approval from three different operators. The COORDINATOR operator must always approve the change, the Service.Desk operator's approval is only necessary if the risk assessment has a value of 3, and the Service Manager operator's approval is only necessary if the risk assessment has a value of 1.

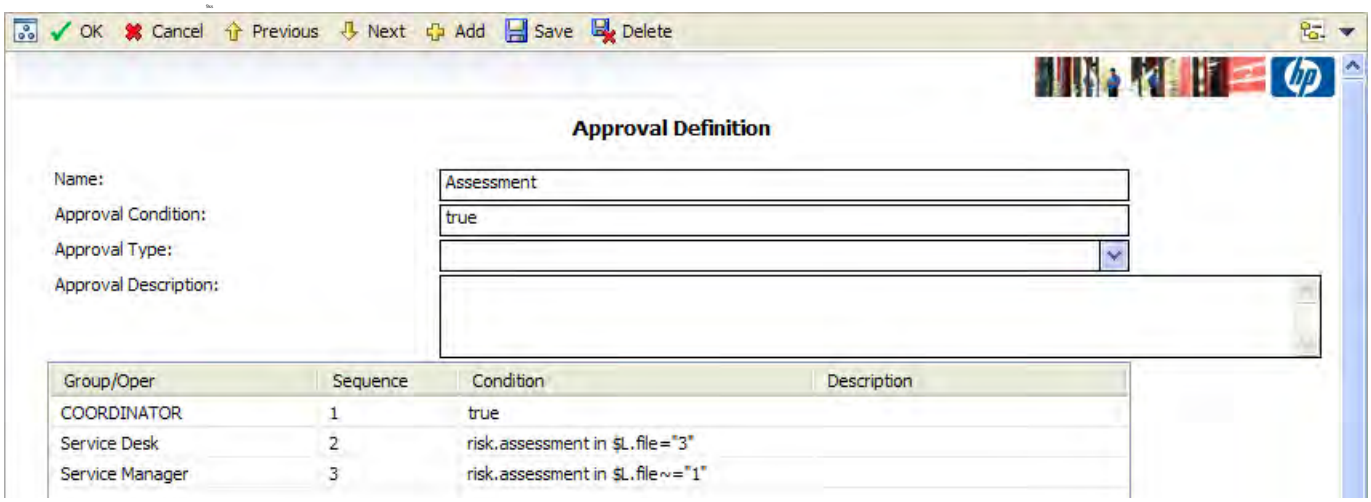

Figure 11-3 Sample Approval Definition record

Service Manager has four approval types that determine how many approvers are required to advance a change to the next phase. Table 11-5 describes the approval types.

Table 11-5 Approval types

Approval type	Description
All must approve	All Groups/Operators defined in the Approval Definition must issue an approval before the change or task can be approved. If only some (but not all) of the Groups/Operators issues an approval, then Service Manager sets the status of the record to "pending." For example, suppose you have three Groups/Operators in an Approval Definition and only one Group/Operator has approved the change. Service Manager sets the status to pending. The Approval table shows one currently pending approval, one future approval, and one completed approval action.
One must approve	The change or task can be approved with one approval from any Group/Operator of the approving group. This is the default value of all Service Manager approvals.
Quorum	The change or task can be approved as soon as a majority of the approving group indicates approval.
All must approve - immediate denial	All Groups/Operators must approve the record. The first denial causes Service Manager to set the status to Deny. All approvers do not need to register their approval action. Otherwise, the record is denied when all Groups/Operators of the approving group issue a denial.

Approval options

Operators with approval rights are enabled to approve, deny, or retract changes and tasks. Table 11-6 explains the approval options.

Table 11-6 Approval options available in Change Management

Approval option	Description
Approve	The approver accepts the need for the change or task, and approves commitment of the resources required to fulfill the request. When all approvals are complete, work begins. When you choose this option, the change request shifts to browse mode, and the retract option is available. If you are not a member of a group with approval rights to this change request, Change Management generates an error message.
Deny	The approver is unwilling to commit the required resources, or does not consider the change or task to be essential. No further approvals are possible until the denial is retracted. An administrative procedure should be set up to handle a denial. If you select deny, a dialog box opens with a prompt to specify the reason for your action. Type an explanation and click OK.
Retract	The approver accepts the need for the change, but is unwilling to commit the resources or perhaps there are technical incidents at the present time. Retract removes a previous approval or denial and resets the change request to pending approved status, which requires a new approval cycle. If you select retract, a dialog box opens with a prompt to specify the reason for your action. Type an explanation and click OK.

Approval delegation

Approval delegation is an optional feature that enables users with approval rights to temporarily delegate their approval authority to another qualified operator. Operators with the “can delegate” option enabled in their application profiles can delegate some or all of their approvals by using the Approval Delegation wizard.

Using the Approval Delegation wizard, an operator can grant another qualified operator the right to temporarily view and act on items in his or her approval queue. The wizard offers the following delegation options:

- Delegate all approvals to another qualified operator
- Delegate approvals from a particular application to another qualified operator
  - Delegate approvals directly assigned to you as an operator
  - Delegate approvals assigned to you as a member of an approval group
- Delegate approvals from a specified start date to a specified end date

You can only delegate to individual operators not groups.

The Approval Delegation wizard enables an operator to create any number of approval delegation combinations, including delegating the same approvals to multiple operators at the same time. Delegators can also update an existing approval delegation to change the delegation start and end dates, as well as change the delegate's name.

Service Manager prevents delegators from deleting past delegations for compliance reasons such as Sarbanes Oxley (SOX). Service Manager tracks all changes to approval delegations using the standard field auditing capability.

When delegates log on to Service Manager, they see both their own and any delegated approvals in their approval list. For security reasons, delegates always retain their original application profiles and operator records. Service Manager determines what temporary rights delegates have when they view or act on an approval.

Change Management tasks

Service Manager change tasks describe the work necessary to complete a particular phase. Work cannot proceed to the next phase until all associated tasks of the current phases are complete. Tasks can be either sequential or parallel. For example, suppose you are in the Change Implementation phase of a hardware change to replace a hard drive. You might have change tasks to back up the old drive, remove the old hard drive, install the new hard drive, test the new hard drive, and restore the data on the new hard drive. In this example, the tasks are sequential because you cannot restore data onto a new drive until you first make a back up of the data and install the new hard drive. Parallel tasks might include determining what backup software to use, determining what hard drive vendor to purchase from, and determining how much effort and risk the hard drive change might take.

Tasks typically include a description of the task, the urgency and priority of the task, task scheduling information, and the task assignment.

Change Management tasks include:

- Opening, assigning, and associating a task with a change.
- Searching for a task.
- Managing task categories, environments, and phases.
- Using the task queue.

Change Management user roles

Table 11-7 describes the responsibilities of the Change Management user roles.

Table 11-7 Change Management user roles

Role	Responsibilities
Change Analyst	• May be involved in the Change Assessment and Planning phase to deliver input to the Change Coordinator when assessing the change impact. • Verifies that tasks are correctly assigned and rejects tasks if needed. • Builds, tests, and implements changes based on the change plan. • Executes the backup plan if required.
Change Approver	• Approve or deny Change when requested. This can be either electronically by using the service management tool or by using a Change Advisory Board (CAB) or Emergency-Change Advisory Board (E-CAB) meeting.
Change Coordinator	• Registers changes and applies the correct change model and change detail. • Schedules changes according to the plan created previously. • Creates the change tasks for building, testing, and implementing a change. • Coordinates the assessment phase of the change and creates change planning based upon the assessment information. • Verifies that the change passed the test criteria. • Verifies that the change is implemented successfully in the production environment. • After implementation, evaluates the change handling and closes the change. • After or during a change implementation failure, activates the remediation plan to return the system to a pre-change state.
Change Manager	• Reviews all changes after the assessment and planning phase and forwards them the right Change Approver. • Organizes Change Advisory Board meeting if necessary. • Updates the change after approval is given. • Periodically reviews changes in a Post Implementation Review and determines and executes follow-up actions. • Coordinates all activities in case the Emergency Change Handling process is triggered.
E-CAB	• Selection of Change Approvers who need to provide approval in case of an Emergency Change
Release Packaging and Build Manager	• Change Analyst who transfers the new release from development to test environment or from test to production environment.This role cannot be fulfilled by the Change Analyst who has built the new release.

Input and output for Change Management

Changes can be triggered and resolved in several ways. Table 11-8 outlines the inputs and outputs for the Change Management process.

Table 11-8 Input and output for Change Management

Input to Change Management	Output from Change Management
• Policy and strategies for change and release • Request for change • Change proposal • Plans (change, transition, release, deployment, test, evaluation, and rendition) • Current change schedule and projected service outage (PSO) • Current assets or configuration items • As-planned configuration baseline • Test results, test report, and evaluation report.	• Rejected Request for Changes (RFCs) • Approved RFCs • Change to a service or infrastructure • New, changed, or disposed assets or CIs • Change schedule • Revised PSO • Authorized change plans • Change decisions and actions • Change documents and records • Change Management reports

Key performance indicators for Change Management

The Key Performance Indicators (KPIs) in Table 11-9 are useful for evaluating your Change Management processes. To visualize trend information, it is useful to graph KPI data periodically. In addition to the data provided by Service Manager, you may need additional tools to report on all of your KPI requirements.

Table 11-9 Key Performance Indicators for Change Management

Title	Description
% of unauthorized changes	Percentage of unauthorized implemented changes in a given time period. A change in the infrastructure without a registered change request is considered unauthorized.
% of incidents caused by changes	Percentage of incidents caused by the implementation of a change in a given time period.
% of emergency changes	Percentage of the total number of closed changes that were emergency changes in a given time period.
% of successful changes	Percentage of the total number of closed changes successfully implemented in a given time period.
% of backed out changes	Percentage of the total number of closed changes for which a remediation plan is activated in a given time period.
% of rejected changes	Percentage of the total number of closed changes rejected in a given time period.
Average time per phase	Average amount of time spent on each of the distinct change phases in a given time period: Change Review, Change Assessment and Planning, Change Approval, Coordinate Change Implementation, and Change Evaluation and Closure.

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included below.

ITIL V3 Key Performance Indicators

The following are ITIL V3 KPIs for Change Management:

- Number of changes implemented to services that met customer requirements (for example, quality/cost/time as expressed as a percentage of all changes).
- Benefits of change expressed as the value of improvements made added to the value of negative impacts prevented or terminated as compared with the costs of the change process.
- Reduction in the number of disruptions to services, defects, and rework caused by inaccurate specification, and poor or incomplete impact assessment.
- Reduction in the number of unauthorized changes.
- Reduction in the backlog of change requests.
- Reduction in the number and percentage of unplanned changes and emergency fixes.
- Change success rate (percentage of changes deemed successful at review, that is, the number of RFCs approved).
- Reduction in the number of changes in which remediation is required.
- Reduction in the number of failed changes.
- Average time to implement based on urgency/priority/change type.
- Incidents attributable to changes.
- Percentage accuracy in change estimate.

COBIT 4.1 Key Performance Indicators

The following are the COBIT 4.1 KPIs for Change Management:

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment.
- Amount of application rework caused by inadequate change specifications.
- Reduced time and effort required to make changes.
- Percent of total changes that are emergency fixes.
- Percent of unsuccessful changes to the infrastructure due to inadequate change specifications.
- Number of changes not formally tracked, reported, or authorized.
- Number of backlogged change requests.
- Percent of changes recorded and tracked with automated tools.
- Percent of changes that follow formal change control processes.
- Ratio of accepted to refused change requests.
- Number of different versions of each business application or infrastructure being maintained.
- Number and type of emergency changes to the infrastructure components.
- Number and type of patches to the infrastructure components.

RACI matrix for Change Management

A Responsible, Accountable, Consulted, and Informed (RACI) diagram or RACI matrix is used to describe the roles and responsibilities of various teams or people in delivering a project or operating a process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. The RACI matrix for Change Management is shown in Table 11-10.

Table 11-10 RACI matrix for Change Management

Process ID	Activity	Change Manager	Service Desk Agent	Incident Manager	Problem Manager	Release Manager	Change Coordinator	Change Approver (or CAB/E-CAB	Change Analyst	Release Packaging and Build Manager
ST 2.1	Change Logging	A	R	R	R	R	R			
ST 2.2	Change Review	A		I	I	I	R			
ST 2.3	Change Assessment and Planning	A	I	I	I	I	R		C/I	C/I
ST 2.4	Change Approval	R/A	I	I	I	I	I	R		
ST 2.5	Coordinate Change Implementation	A	I	I	I	I	R		R	R
ST 2.6	Change Evaluation and Closure	R/A	C	C	C	C	R		C	C
ST 2.7	Emergency Change Handling	R/A		C/I				R	R	R

12 Change Management Workflows

Change Management controls the process to request, manage, approve, and control changes that modify your organization infrastructure. This managed infrastructure includes assets, such as network environments, facilities, telephony, and resources. For user requests for products and services, refer to Request Management.

Change Management automates the approval process and eliminates the need for memos, email, and phone calls.

The Change Management process consists of the following processes, which are included in this chapter:

Change Logging (process ST 2.1)

An individual or organizational group that requires a change can initiate a Request for Change (RFC). Change requests can be initiated as part of a variety of management processes, including User Interaction Management, Incident Management, Problem Management, and Release Management. Each RFC must be registered in an identifiable way. HP Service Manager provides change templates that standardize and speed up the Change Logging process.

The following user roles can perform Change Logging:

- Service Desk Agent
- Problem Manager
- Change Coordinator
- Release Manager

Details for this process can be seen in the following figure and table.

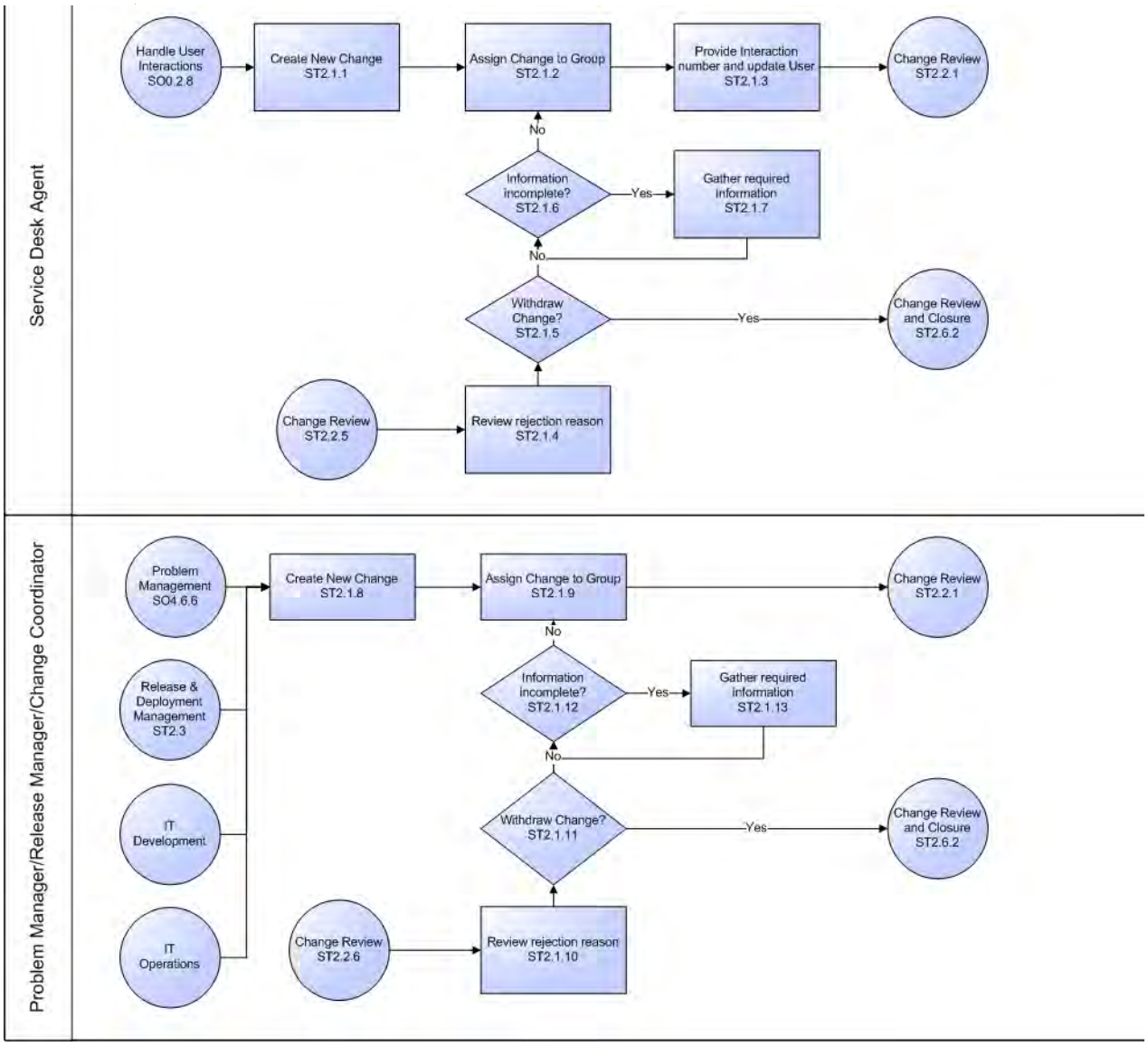

Figure 12-1 Change Logging workflow

Table 12-1 Change Logging process

Process ID	Procedure or Decision	Description	Role
ST 2.1.1	Create new change	This procedure starts when the Service Desk Agent is working on an open-idle interaction in the category “Request for Change” and escalates it by creating a change request in the tool.	Service Desk Agent
ST 2.1.2	Assign change to group	Based on the RFC details (or on the comment listed in the rejection reason field) the Service Desk Agent assigns the change to the correct support group.	Service Desk Agent
ST 2.1.3	Provide interaction number and update user	When a change has been created from an interaction on first intake, the user receives an interaction number and is updated with the actions performed by the Service Desk Agent. When the interaction has been created by using self-service, the user is updated with the interaction status and actions. The change is then sent to the Change Review procedure (ST 2.2.1).	Service Desk Agent
ST 2.1.4	Review rejection reason	The Change Coordinator has rejected the change request when reviewing the content. The Service Desk Agent checks the rejection reason and the actions defined.	Service Desk Agent
ST 2.1.5	Withdraw change	Based on the rejection reason, it may be decided that the change request is not valid anymore and needs to be withdrawn (for example, if it is not feasible to deliver the requested information). If the change is withdrawn, the Change Review and closure process is started (ST 2.6.2). If the change is not withdrawn, go to ST 2.1.6.	Service Desk Agent
ST 2.1.6	Information incomplete?	Is the change request rejected because it did not contain all necessary information? If yes, continue with ST 2.1.7. If no, go to ST 2.1.2.	Service Desk Agent
ST 2.1.7	Gather required information	The Service Desk Agent contacts the change initiator and gathers and records the required information.	Service Desk Agent
ST 2.1.8	Create new change	• The Problem Manager escalates a known error to a change request • The Release Manager creates a new change request to implement a new release • The Change Coordinator creates a new change request based on the direct request of an IT specialist from operations or development. If known, the correct change model can immediately be selected. If unknown, choose the “Default Change” Change Model.	Problem Manager/ Release Manager/ Change Coordinator
ST 2.1.9	Assign change to group	Based on the RFC details (or the comment listed in the rejection reason field) the Problem Manager/Release Manager/Change Coordinator assigns the change to the correct support group. The change is then sent to the Change Review process (ST 2.2.1).	Problem Manager Release Manager Change Coordinator
ST 2.1.10	Review rejection reason	The Change Coordinator has rejected the change request when reviewing the content. The Problem Manager/Release Manager/ Change Coordinator checks the rejection reason and the actions defined.	Problem Manager Release Manager Change Coordinator

Table 12-1 Change Logging process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 2.1.11	Withdraw change	Based on the rejection reason, it may be decided that the change request is not valid anymore and needs to be withdrawn (for example, if it is not feasible to deliver the requested information). If the change is withdrawn, the Change Review and closure process is started (ST 2.6.2). If the change is not withdrawn, go to ST 2.1.12.	Problem Manager Release Manager Change Coordinator
ST 2.1.12	Information incomplete?	Is the change request rejected because it did not contain all necessary information? If yes, continue with ST 2.1.13 If not, go to ST 2.1.8.	Problem Manager/ Release Manager/ Change Coordinator
ST 2.1.13	Gather required information	The Problem Manager/Release Manager/Change Coordinator gathers and records the required information.	Problem Manager/ Release Manager/ Change Coordinator

Change Review (process ST 2.2)

After a change request is logged, the Change Coordinator verifies that the request is logical, feasible, necessary, and complete. If more information is needed, the Change Coordinator will request that the initiator update the request. The Change Coordinator also checks to see if the change has already been previously submitted and rejected. If a requested change does not meet the requirements, the Change Coordinator rejects the change and communicates the reason for the rejection to the change initiator. The Change Review process is performed by the Change Coordinator.

Details for this process can be seen in the following figure and table.

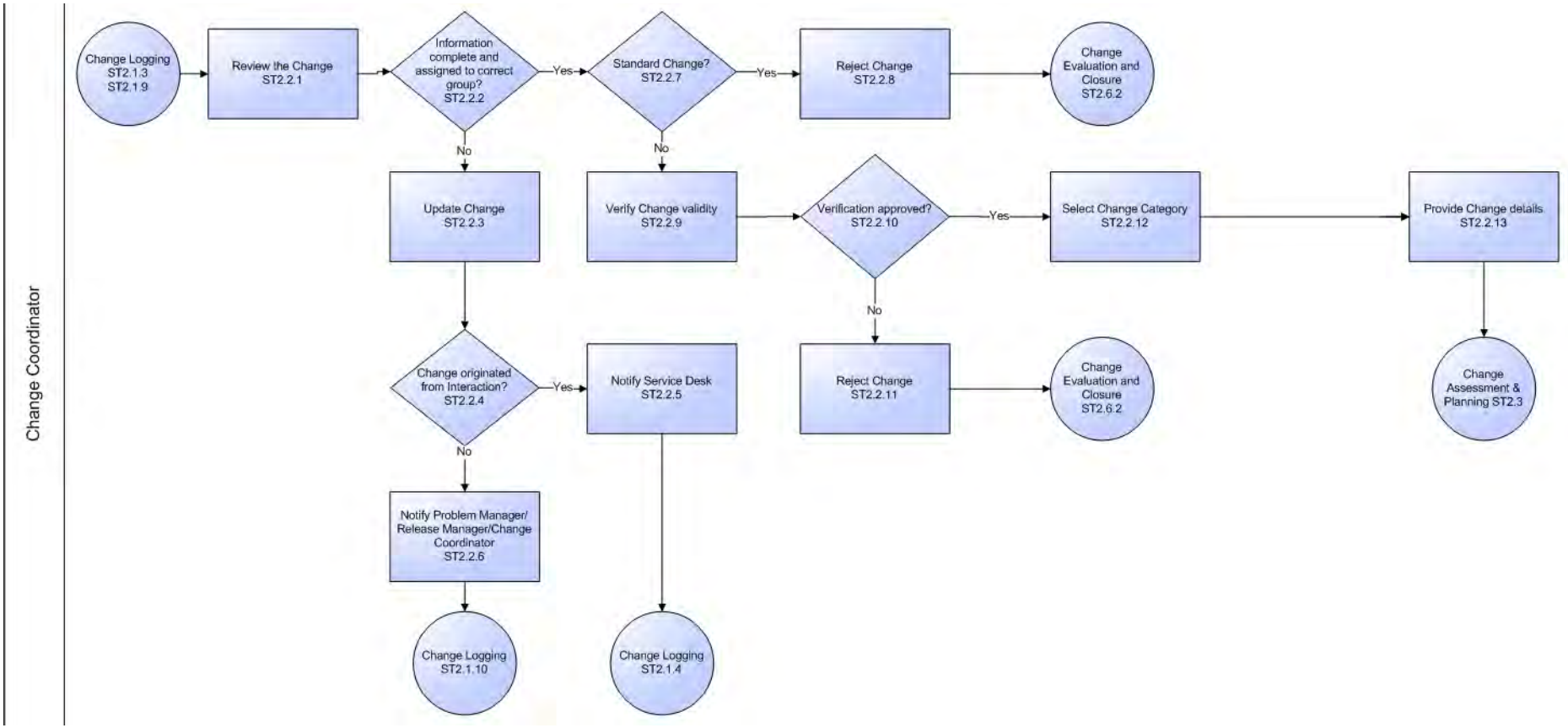

Figure 12-2 Change Review workflow

Table 12-2 Change Review process

Process ID	Procedure or Decision	Description	Role
ST 2.2.1	Review the change	The Change Coordinator selects a change from the new change request queue and starts reviewing the change information.	Change Coordinator
ST 2.2.2	Information complete and assigned to correct group?	The Change Coordinator verifies that the required information in the change is available and that the change has been assigned to the correct support group. If yes, continue with ST 2.2.7. If no, go to ST 2.2.3.	Change Coordinator
ST 2.2.3	Update change	The Change Coordinator updates the change and states the reason that the change is returned to the request initiator.	Change Coordinator
ST 2.2.4	Change originated from interaction?	The Change Coordinator determines if the change request was created from an interaction or from a problem ticket. If it was created from an interaction record, the rejected change request is sent back to the Service Desk (ST 2.2.5). If it was created from a problem ticket, the rejected change is sent back to the Problem Manager (ST 2.2.6).	Change Coordinator
ST 2.2.5	Notify Service Desk	The Change Coordinator notifies the Service Desk of the reason that the change is returned, including any required actions.	Change Coordinator
ST 2.2.6	Notify Problem Manager/Release Manager/Change Coordinator	The Change Coordinator notifies the Problem Manager/Release Manager/Change Coordinator of the reason that the change is returned, including any required actions.	Change Coordinator
ST 2.2.7	Standard change?	The Change Coordinator verifies if this is a request, which should be handled by using the request fulfillment process, or if it should be verified as a change request that is feasible and necessary. If this request can be handled using the request fulfillment process, continue with ST 2.2.8. If not, go ST 2.2.9.	Change Coordinator
ST 2.2.8	Reject change	The Change Coordinator rejects the change and updates the record with a rejection reason. The change is then sent to the Change Evaluation and Closure process (ST 2.6.2).	Change Coordinator
ST 2.2.9	Verify change is valid	The Change Coordinator verifies that the change is logical, feasible, and necessary, and makes sure that it does not contradict company standards and policies and that it has not previously been initiated and rejected.	Change Coordinator
ST 2.2.10	Verification approved?	If the change passes the validity criteria, continue with ST 2.2.12. If not, go to ST 2.2.11.	Change Coordinator
ST 2.2.11	Reject change	The Change Coordinator rejects the change and updates the record with a rejection reason. The change is then sent to the Change Evaluation and Closure process (ST 2.6.2).	Change Coordinator
ST 2.2.12	Select change category	The change request has initially been created from a default category. The Change Coordinator now selects the appropriate change category.	Change Coordinator
ST 2.2.13	Provide change details	The change is completed with other information that was not automatically provided from the change category.	Change Coordinator

Change Assessment and Planning (process ST 2.3)

For all normal changes, the Change Coordinator assesses the need for a change based on answers to the following questions:

- Who is the requestor that initiated the need for the change?
- What is the reason for the change?
- What is the result required from the change?
- What are the risks involved in the change?
- What resources are required to deliver the change?
- Who is responsible for the build, test, and implementation of the change?
- What is the relationship between this change and other changes?

Based on the answers to these questions, the change is categorized, prioritized, and planned, and then a remediation plan is developed.

The Change Review process is performed by the Change Coordinator.

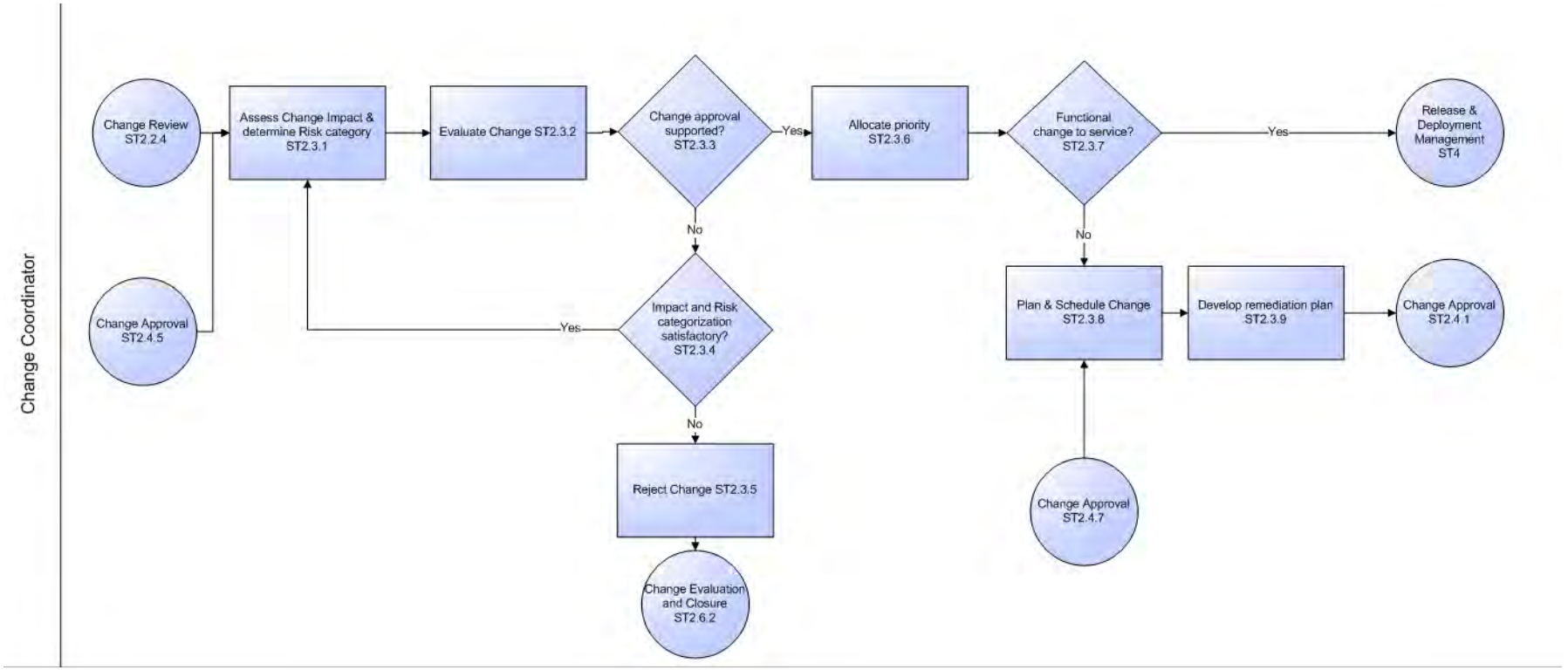

Figure 12-3 Change Assessment and Planning workflow

Table 12-3 Change Assessment and Planning process

Process ID	Procedure or Decision	Description	Role
ST 2.3.1	Assess change impact and determine risk category	When conducting the impact and resource assessment for changes, the Change Coordinator considers the following relevant items: • Impact that the change will make on the customer's business operation • Effect on the infrastructure and customer service • Impact on other services that run on the same infrastructure (or on projects) • Impact on non-IT infrastructures within the organization • Effect of not implementing the change • The IT, business, and other resources required to implement the change including the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required • The current change schedule (CS) and projected service outage (PSO) • Additional ongoing resources required if the change is implemented • Impact on the continuity plan, capacity plan, security plan, regression test scripts, data and test environment, and Service Operations practices. If needed, the Change Coordinator can include business owners and technical analysts' requirements and probability of risk. The appropriate risk level can then be calculated or measured and included in the process and decision of making the change. Based on the impact and the probability of the change to occur, the risk category is determined.	Change Coordinator
ST 2.3.2	Evaluate change	The Change Coordinator contacts the Change Analysts (for example, IT specialists, security officer, System Administrator) after the change assessment. The Change Analysts evaluate the information and indicate whether they support approval of the change.	Change Coordinator
ST 2.3.3	Change Approval supported?	Based on the change evaluation, the Change Coordinator determines whether the change is supported for approval or not. If no, continue with ST 2.3.4. If yes, continue with ST 2.3.6.	Change Coordinator
ST 2.3.4	Impact and risk categorization unsatisfactory?	Has the change not been approved because the impact and risk categorization is not satisfactory? If yes, go back to ST 2.3.1. If no, continue with ST 2.3.5.	Change Coordinator
ST 2.3.5	Reject change	The Change Coordinator rejects the change and updates the change with a rejection reason. The change is then sent for the Change Evaluation and Closure process (ST 2.6.2).	Change Coordinator
ST 2.3.6	Allocate priority	The Change Coordinator considers the impact and urgency of a change to set the priority. The priority establishes the order in which changes are processed.	Change Coordinator

Table 12-3 Change Assessment and Planning process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 2.3.7	Functional change to service?	Does this change concern a functional change of the service? If yes, Release and Deployment Management is needed for the clustering, approval, build, and test. Go to the Release and Deployment management process (ST4). If no, continue with ST 2.3.8.	Change Coordinator
ST 2.3.8	Plan and schedule change	The Change Coordinator carefully plans and schedules the change. A detailed change plan is created, which indicates the activities that will need to be performed to implement the change. The change plan can be visualized in change tasks. If a very detailed plan is created, it might be more appropriate to attach the plan to the change as an attachment. The Planned Change Start and End Date need to be filled in to publish the change on the change calendar. Before scheduling the change, the change calendar should be checked to verify that there are no conflicting changes in the scheduled period. If possible, the change should be scheduled in the maintenance window for the impacted service(s), as agreed in the SLA.	Change Coordinator
ST 2.3.9	Develop remediation plan	The Change Coordinator develops a remediation plan that contains an alternate remediation scenario that describes how to undo the change.	Change Coordinator

Change Approval (process ST 2.4)

Every change requires a formal authorization from a change authority, which may be a role, person, or group of people. The levels of authorization for a particular type of change are judged by the type, size, or risk of the change.

Details for this process can be seen in the following figure and table.

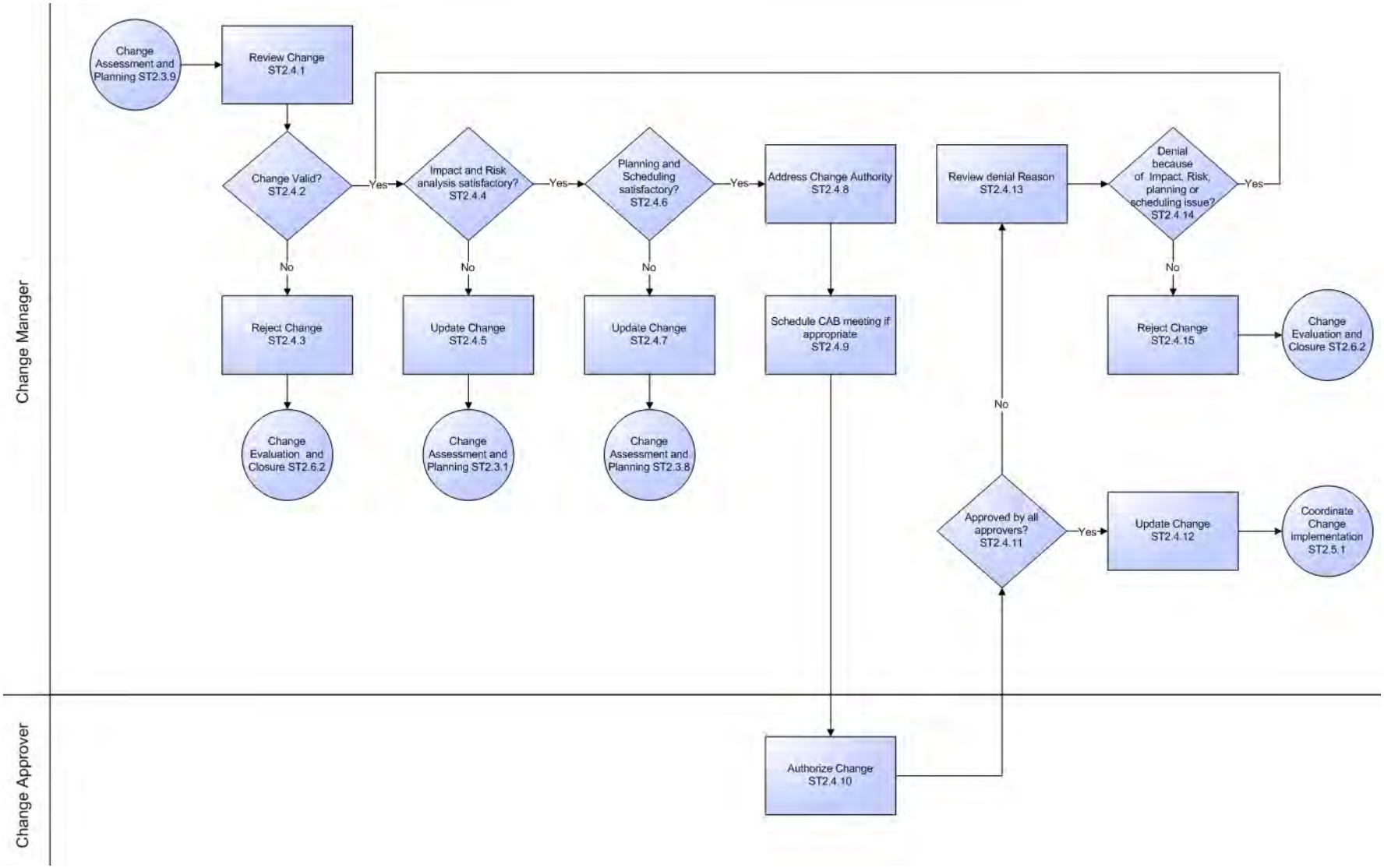

Figure 12-4 Change Approval workflow

Table 12-4 Change Approval process

Process ID	Procedure or Decision	Description	Role
ST 2.4.1	Review change	The Change Manager verifies that the change is logical, feasible, and necessary. The Change Manager also makes sure that the change does not conflict with company standards and policies, and checks to see if the proposed change has been proposed and rejected in the past. This verification step is typically also performed by the Change Coordinator at an earlier step in the process. However, for segregation of duties reasons, be sure that changes are validated again by the Change Manager.	Change Manager
ST 2.4.2	Change valid?	If yes, go to ST 2.4.4. If no, go to ST 2.4.3.	Change Manager
ST 2.4.3	Reject change	If the change is invalid, the change is rejected by the Change Manager and is input for the Change Evaluation and Closure process.	Change Manager
ST 2.4.4	Impact and risk analysis satisfactory?	If yes (that is, assessment of change impact and analysis and determination of risk category is satisfactory), go to ST 2.4.6. If no, go to ST 2.4.5.	Change Manager
ST 2.4.5	Update change	Update the change with the remarks about the impact and risk analysis, and then request that the Change Coordinator update the change.	Change Manager
ST 2.4.6	Planning and scheduling satisfactory?	If yes, go to ST 2.4.8. If no, go to ST 2.4.7.	Change Manager
ST 2.4.7	Update change	Update the change with the remarks about the planning and scheduling, and then request that the Change Coordinator update the change.	Change Manager
ST 2.4.8	Address change authority	The Change Manager determines the level of authorization based on the type, size, or risk of the change. The Change Manager then selects the approvers required for each change. At minimum, the Group Manager of the affected Service and the CI Group Manager of the affected CI(s) should approve the change.	Change Manager
ST 2.4.9	Schedule CAB meeting if appropriate	The Change Manager determines whether a CAB meeting should be scheduled to discuss the change approval, or if instead the change can be authorized via email or the Change Management registration system.	Change Manager
ST 2.4.10	Authorize change	The Change Approver selects the change that he or she must approve, checks the change content, and then either approves or denies the change. If the Change Approver has questions to ask prior to granting approval, the Change Approver directs questions to the Change Coordinator. If the change is denied, the Change Approver must fill in a denial reason.	Change Approver
ST 2.4.11	Approved by all approvers?	When all approvers have authorized the change, the Change Manager verifies that the change has been approved by all. If yes, continue with ST 2.4.12. If no, go to ST 2.4.13.	Change Manager

Table 12-4 Change Approval process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 2.4.12	Update change	The Change Manager updates the change with the approval information and passes the change to the Change Coordinator for implementation.	Change Manager
ST 2.4.13	Review denial reason	Review the reasons that a Change Approver has denied authorization for the change.	Change Manager
ST 2.4.14	Denial because of an impact, risk, planning, or scheduling issue?	If yes, go to ST 2.4.4. If no, go to ST 2.4.15.	Change Manager
ST 2.4.15	Reject change	The Change Manager rejects the change based on approval results. The Change Manager fills in a rejection reason and the change is sent to the Change Evaluation and Closure process.	Change Manager

Coordinate Change Implementation (process ST 2.5)

Authorized change requests should be passed to the relevant technical groups for building, testing, and implementing the change. The Change Coordinator schedules tasks for the build, test, and implementation phases and assigns those tasks to the responsible Change Analysts. Change Management is responsible for ensuring that changes are implemented as scheduled. The actual implementation of authorized changes is performed by Change Analysts in the specialist groups.

Details for this process can be seen in the following figure and table.

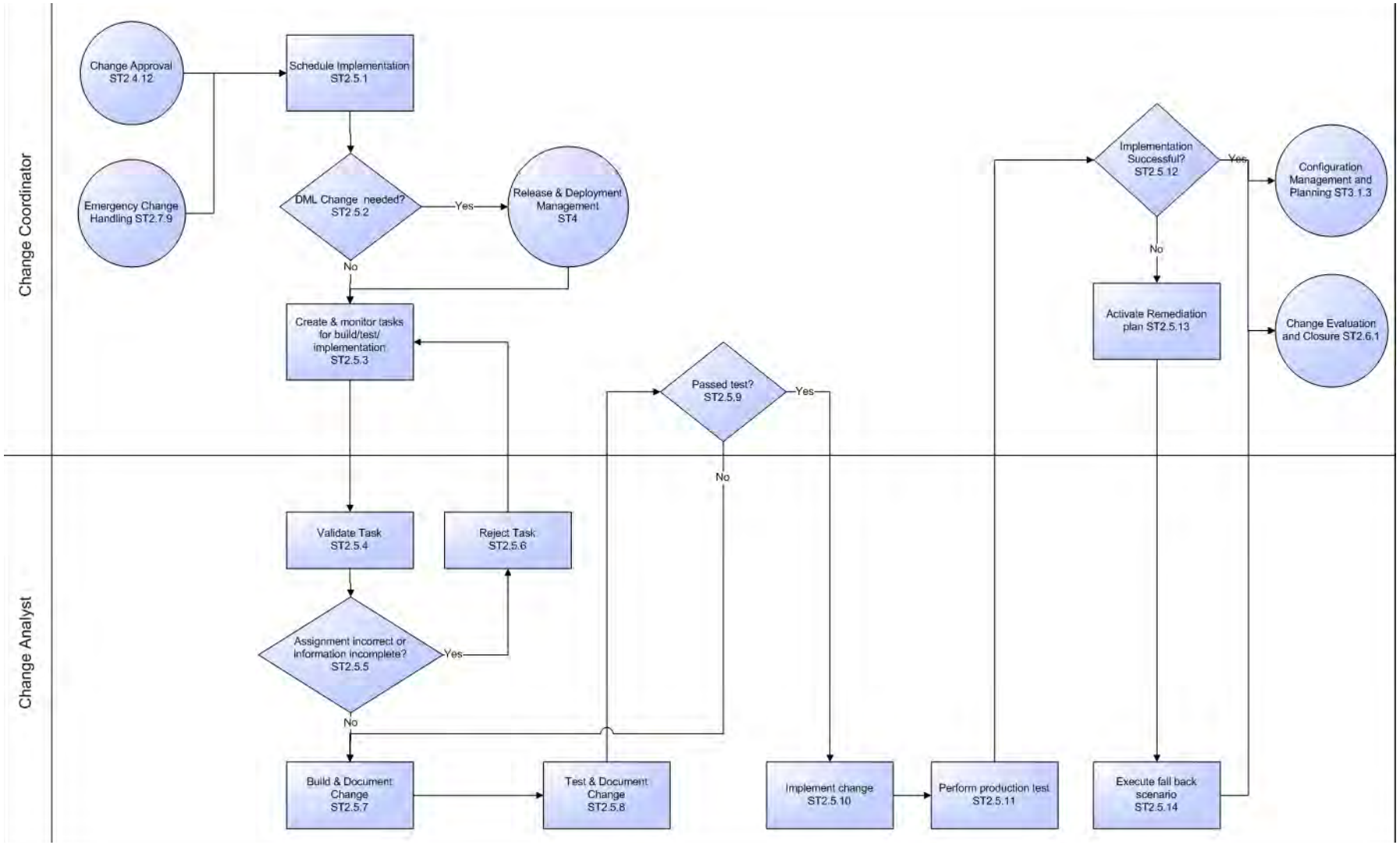

Figure 12-5 Coordinate Change Implementation workflow

Table 12-5 Coordinate Change Implementation process

Process ID	Procedure or Decision	Description	Role
ST 2.5.1	Schedule implementation	The Change Coordinator schedules managing the change, according to the plan created previously.	Change Coordinator
ST 2.5.2	Definitive Media Library change needed?	Does this particular change require a change in the Definitive Media Library (for example, changes related to software development or a new type of hardware)? If no, continue with ST 2.5.3. If yes, continue to the Definitive Media Library to make the change, and then forward the change to the release and deployment process where the following activities will be executed: • Plan the release • Update the Definitive Media Library • Communicate with stakeholders • Build release • Test release • Document release After release and deployment management has finished the release package, the change is returned to the Change Management process.	Change Coordinator
ST 2.5.3	Create and monitor tasks for build, test, and implementation	The Change Coordinator creates the change tasks for building, testing, and implementing the change. All tasks are scheduled and assigned to the scheduled Change Analyst. Then the Change Coordinator monitors the progress of the change tasks and the change.	Change Coordinator
ST 2.5.4	Validate task	The Change Analyst verifies that the change task has been correctly assigned and that the information is complete to execute the change task.	Change Analyst
ST 2.5.5	Assignment incorrect or information incomplete?	If the assignment is incorrect or information incomplete, go to ST 2.5.6. If not, go to ST 2.5.7.	Change Analyst
ST 2.5.6	Reject task	The change task is rejected and returned to the Change Coordinator.	Change Analyst
ST 2.5.7	Build and document change	The Change Analyst builds or configures the change, as scheduled. It is important that all changes in the infrastructure are well documented. When finished building the change, the Change Analyst sends the change for testing.	Change Analyst
ST 2.5.8	Test and document change	All hardware changes, software changes, and new releases must be tested before implementing them in production. Test plans must be available to support the test activities, and the test results must be documented.	Change Analyst
ST 2.5.9	Passed test?	The Change Coordinator verifies that the change has passed the test criteria. If yes, the change is authorized to be implemented in the production environment, go to ST 2.5.10. If not, go to ST 2.5.7.	Change Coordinator

Table 12-5 Coordinate Change Implementation process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 2.5.10	Implement change	The Change Analyst implements the change in the production environment, according to the change implementation schedule.	Change Analyst
ST 2.5.11	Perform production test	Immediately after implementing the change in the production environment, perform verification tests to determine if the change implementation was successful.	Change Analyst
ST 2.5.12	Implementation successful?	The Change Coordinator verifies whether or not the change has been successfully implemented in the production environment. If the change has not been successfully implemented in the production environment, go to step 2.5.13 to activate the remediation plan. An example of an unsuccessful change implementation is if a change causes a severe disruption of the changed service or services. If the change is successfully implemented in the production environment, the change is passed to the Change Evaluation and Closure process ST 2.6.1. The change is also passed to the Configuration Management Planning process ST 3.1.3 to update the Configuration Management System (CMS). A change cannot be closed until all changes on the involved CIs have been registered in the Configuration Management System (CMS).	Change Coordinator
ST 2.5.13	Activate remediation plan	After or during the change implementation failure, the Change Coordinator activates the remediation plan to return the system to the prechange state.	Change Coordinator
ST 2.5.14	Execute fallback scenario	The Change Analyst is the expert who executes the fallback scenario and rolls back the change.	Change Analyst

Change Evaluation and Closure (process ST 2.6)

After a change is completed, the results must be reported for evaluation to those responsible for managing changes, and then presented for stakeholder agreement. This process includes the closing of related user interactions, incidents, and known errors.

A change evaluation (for example, a post-implementation review, or PIR) is performed to confirm that:

- the change meets its objectives
- the change initiator and stakeholders are satisfied with the results
- unanticipated effects have been avoided.
- Lessons learned are incorporated into future changes.

The Change Review process is performed by the Change Coordinator and the Change Manager.

Details for this process can be seen in the following figure and table.

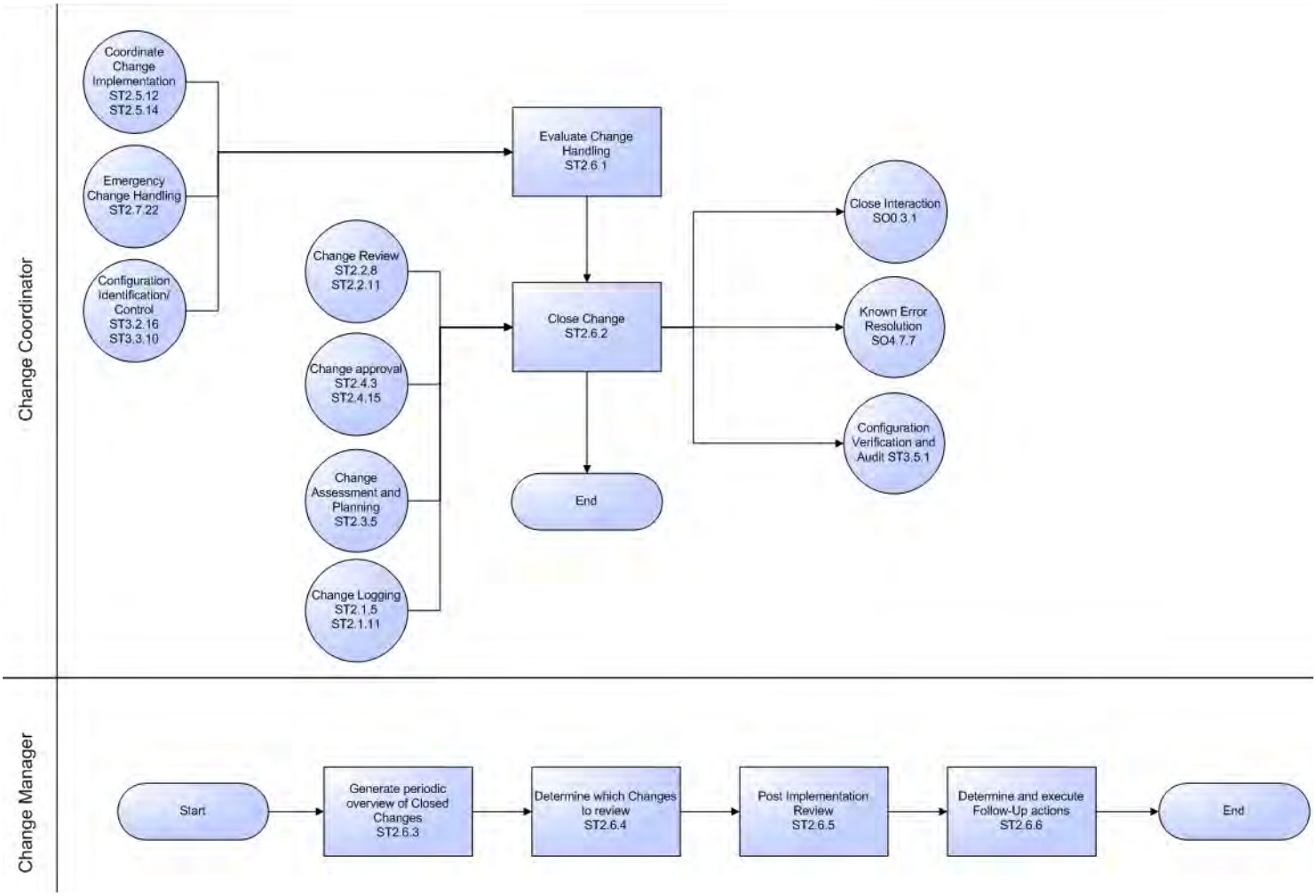

Figure 12-6 Change Evaluation and Closure workflow

Table 12-6 Change Evaluation and Closure process

Process ID	Procedure or Decision	Description	Role
ST 2.6.1	Evaluate change handling	After implementation of the change, the Change Coordinator verifies that the change was handled correctly and that the administration of the change is complete. The Change Coordinator also reviews change handling to verify that all related tickets are still correct.	Change Coordinator
ST 2.6.2	Close change	The Change Coordinator updates the change request and closes the change. The change request is now closed and all change initiators receive a notification that the related change is successfully implemented.	Change Coordinator
ST 2.6.3	Generate periodic overview of closed changes	The Change Coordinator generates an overview of all changes that have been closed since the last review.	Change Coordinator
ST 2.6.4	Determine which changes to review	The Change Manager then narrows the overview to a list of changes that require reviewing.	Change Manager
ST 2.6.5	Post Implementation Review (PIR)	Change Manager must review certain changes after a predefined period. This process involves CAB members and is part of the CAB agenda. The purpose of the review is to establish the following: • Change has had the desired effect and met its objectives. • Users, customers, and other stakeholders are satisfied with the results, and any shortcomings are identified. • There are no unanticipated or undesirable side effects to functionality, service levels, or warranties (for example, availability, capacity, security, performance, and costs). • Resources used to implement the change were as planned. • Release and deployment plan worked correctly (recorded information includes comments from the implementers). • Change was implemented on time and to cost. • Remediation plan functioned correctly, if required.	Change Manager
ST 2.6.6	Determine and execute follow-up action	Based on the outcome of the Post Implementation Review, the Change Manager defines an action list and starts the execution of defined actions.	Change Manager

Emergency Change Handling (process ST 2.7)

Emergency changes can only be initiated from within the Incident Management process. They should be used only to repair an IT service error that is negatively impacting the business at a high level of severity. Changes that are intended to make an immediately required business improvement are handled as normal changes, although they may be assigned a high priority based on the urgency of the required business improvement.

The emergency change process follows the normal change process, except for the following:

- Approval is given by the Emergency Change Approval Board (E-CAB) rather than waiting for a regular CAB meeting.
- Testing may be reduced, or in extreme cases eliminated, if doing so is considered necessary to deliver the change immediately.
- Updating of the change request and configuration data may be deferred, typically until normal working hours.

If the E-CAB decides that an emergency change can be handled as a normal change, the emergency change is recategorized and implemented by using the normal change process.

The following user roles are involved in Emergency Change Handling:

- Change Manager
- Change Analyst
- E-CAB
- Release Packaging and Build Manager

Details for this process can be seen in the following figure and table.

Figure 12-7 Emergency Change Handling workflow

Table 12-7 Emergency Change Handling process

Process ID	Procedure or Decision	Description	Role
ST 2.7.1	Discuss and determine change requirements	The Change Manager discusses the requirements for the emergency change in cooperation with the Incident Manager.	Change Manager
ST 2.7.2	Determine change impact and risk category	The change impact and risk category is determined the same way as a normal change request, except that it is designated as high priority.	Change Manager
ST 2.7.3	Organize emergency CAB meeting	The Change Manager calls the Emergency CAB (E-CAB) to authorize the change. The E-CAB consists of members authorized to make decisions about high impact emergency changes.	Change Manager
ST 2.7.4	Authorize change	The E-CAB members authorize the change.	E-CAB
ST 2.7.5	Approved by E-CAB?	Has the emergency change been approved by the E-CAB members? If yes, continue with ST 2.7.8. If no, go to ST 2.7.6.	Change Manager
ST 2.7.6	Additional requirements set by E-CAB?	The Change Manager notes whether E-CAB denies a proposed emergency change due to extra requirements for the Change Management process. If there are extra requirements, go to ST 2.7.1. If no, go to ST 2.7.7.	Change Manager
ST 2.7.7	Reject change	The Change Manager rejects the emergency change and sends it back to the Incident Manager.	Change Coordinator
ST 2.7.8	Handle as emergency change?	Has the E-CAB decided to handle this change as an emergency change? If yes, go to ST 2.7.10. If no, go to ST 2.7.9.	Change Manager
ST 2.7.9	Recategorize and update change	The Change Manager recategorizes the change as a normal change and updates the change with all relevant information. Because the change has already been approved by the E-CAB, the Coordinate Change Implementation phase can begin. The assigned Change Coordinator is notified.	Change Manager
ST 2.7.10	Definitive Media Library change needed?	Does this emergency change require a change in the Definitive Media Library (DML)? If yes, go to ST 2.7.12. If no, continue with step ST 2.7.11.	Change Manager
ST 2.7.11	Implement change	The Change Analyst implements the change in the production environment with the highest priority.	Change Analyst
ST 2.7.12	Build release in development environment	The Change Analyst builds a new release with the highest priority. When the Change Analyst is finished, the new release is sent to the Release Packaging and Build Manager.	Change Analyst
ST 2.7.13	Transfer release to test environment	The Release Packaging and Build Manager transfer the new release to the test environment and update the (CMS) or the Definitive Media Library. For compliance reasons, this role should not be performed by the Change Analyst who performs the build.	Release Packaging and Build Manager
ST 2.7.14	Test release	The Change Analyst tests the new release within the set time frame.	Change Analyst

Table 12-7 Emergency Change Handling process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 2.7.15	Test successful?	The Change Analyst accepts the new release and determines if it can be released for transfer to the production environment. If yes, go to ST 2.7.16. The Change Analyst notifies the Release Packaging Manager and Build Manager to transfer the release to the production environment. If no, go back to ST 2.7.12.	Change Analyst
ST 2.7.16	Transfer release to production environment	The Release Packaging and Build Manager transfers the new release to the production environment and updates the status of the new release in the Definitive Media Library.	Release Packaging and Build Manager
ST 2.7.17	Perform test	After implementing the emergency change in production, the Change Analyst performs a quick test to verify that the error has been resolved and has not triggered any other errors.	Change Analyst
ST 2.7.18	Change successful?	The Change Analyst determines if the change was successful or not. If yes, continue with ST 2.7.21. If no, go to ST 2.7.19 to start the rollback process.	Change Analyst
ST 2.7.19	Roll back change	The Change Manager decides to start the rollback procedure.The Change Analyst follows the rollback plan to restore the production environment to its prechange state.	Change Analyst
ST 2.7.20	Inform Incident Manager	The Change Manager informs the Incident Manager about the unsuccessful change implementation and returns the emergency change to the Incident Escalation process.	Change Manager
ST 2.7.21	Inform Incident Manager and Change Manager, and then close the incident ticket	The Change Analyst informs the Incident Manager and the Change Manager about the successfully implemented emergency change. If the Incident Manager agrees, the related incident ticket is closed.	Change Analyst
ST 2.7.22	Handle emergency change request	The Change Manager updates the emergency change request with all relevant information and closes the change phases where appropriate and assigns the change tasks to update the Definitive Media Library/CMS or to have the change activities registered. Then the emergency change is passed to the Change Evaluation and Closure process. Typically this comes after the change implementation.	Change Manager

13 Change Management Details

HP Service Manager uses the Change Management application to enable the Change Management process. The main function of Change Management is to standardize the methods and processes a business organization uses to plan and implement changes. Change Management records all changes to service assets and configuration items in the Configuration Management System (CMS).

In Change Management, the Change Manager sends the change requests to the correct approvers and coordinates Emergency Change Handling, the Change Approver and approves or denys the change request, the Change Coordinator plans the implementation of the change and verifies that the change has been completed satisfactorily, and the Change Analyst implements the change.

This section describes selected Change Management fields in the out-of-box Service Manager system.

Topics in this section include:

Change Management form after escalation from a known error

The following picture shows a new change request escalated from a known error record in Problem Management. As with any new change, you must provide the required fields before you can save it. See Change Management form details on page 183 for a list and description of the fields on this form.

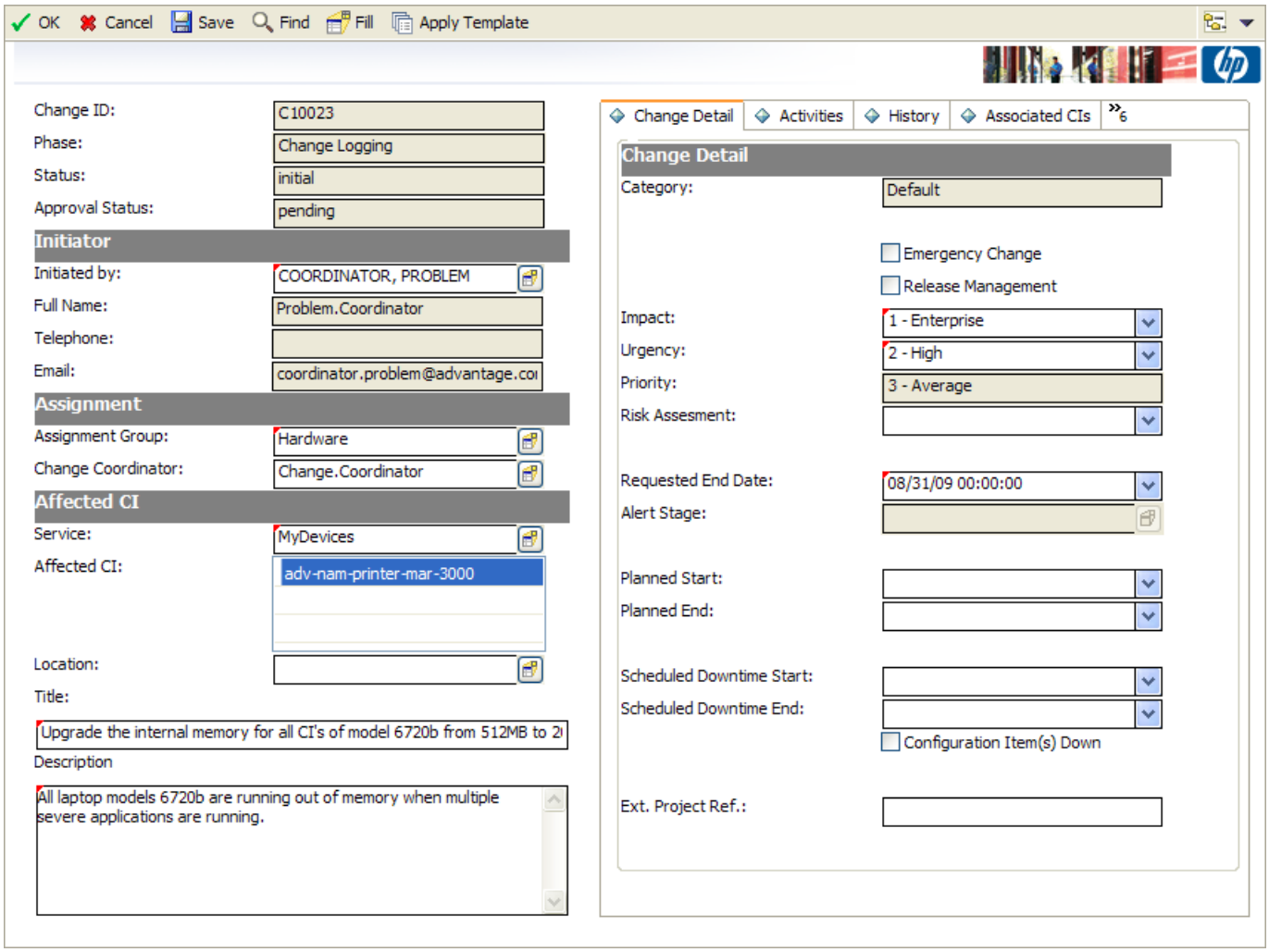

Figure 13-1 Change Management form after escalation from a known error

Change Management form details

The following table identifies and describes some of the features on the Change Management forms.

Table 13-1 Change Management field descriptions

Label	Description
Change ID	This is a system-generated field assigned when the change is opened.
Phase	This is a system-generated field that specifies the name of the current phase of the change. See Change Management phases on page 148 for a list of the phases associated with the various categories.
Status	This is a system-generated field that specifies the status of the change with the phase. These statuses are available out-of-box: • Initial - the change request is open • Waiting - the previous change phase has been closed and the next phase is waiting to be opened • Reopened - the change was previously closed and then reopened • Closed - the change request has been closed
Approval Status	This is a system-generated field that defines the global approval status for the change, not for a single approval. The system sets this field depending on current approvals and the approval type defined for the module. These approval statuses are available out-of-box: • Pending • Approved • Denied
Initiator Initiated by	The name of the user requesting the change. This is a required field.
Initiator Full Name	This is a system-generated field that the system populates based on the contents of the Initiated by field.
Initiator Telephone	This is a system-generated field that the system populates based on the contents of the Initiated by field.
Initiator Email	This is a system-generated field that the system populates based on the contents of the Initiated by field.

Table 13-1 Change Management field descriptions (cont'd)

Label	Description
Assignment Assignment Group	The group assigned to work on the change. For a description of this field see the Assignment Group field description in (Incident Management form details on page 86) as this field functions similarly. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. Tip: You may want to change the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager This is a required field.
Assignment Change Coordinator	The name of the person responsible for coordinating the implementation of the change. Each Change Coordinator may belong to several assignment groups. Each group can have just one Change Coordinator. This is a required field.
Affected CI Service	Specifies the service affected by the change. This is a system-generated field and is prepopulated when a change request is created from an interaction. This is a required field.
Affected CI Affected CI	The list of Configuration Items (CIs) affected by the change. The system pre-populates this field when a change request is created from an incident or known error. Users can add additional CIs.
Location	Specifies the location for the change. The system pre-populates this field the change is created by escalating an interaction.
Title	Provides a short description of the change. This is a required field.
Description	Provides a more detailed description of the change. This is a required field.
Change Detail > Category	This is a system-generated field that classifies the type of change. The Default and Unplanned Change categories are used for changes opened in the background; they are available to Change Managers and System Administrators, but not to regular users. The out-of-box categories are described in Change Management categories on page 147.

Table 13-1 Change Management field descriptions (cont'd)

Label	Description
Change Detail > Emergency Change	When checked, the system handles the change according to the emergency change process. The system adds the ECAB approval group requirement and this allows the change to skip some approvals and phases to make the change happen sooner. An emergency change skips the Change Review and Change Assessment and Planning phases after the phase Change Logging closes. Emergency changes go directly to the phase Prepare for Change Approval. The system also adds the Emergency Group Approval to the Change Approval phase and creates an activity record that shows "This change is logged as an Emergency Change" in the Activities > Historic Activities tab. If a change later becomes an emergency, the activity records notes that "This change has become an Emergency Change." There are also notifications to the Change Manager every time there is an activity (open, update or closure of an emergency change) **Note:** An Emergency Change is not the same as an Unplanned Change.
Change Detail > Release Management	When checked, the system manages this change with the Release Management module.
Change Detail > Impact	This field is prepopulated with data from an incident when a change is created from and incident. It specifies the impact the problem has on the business. The impact and the urgency are used to calculate the priority. These impacts are available out-of-box: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User The out-of-box data is the same as Interaction Management, Problem Management, and Incident Management. This is a required field.
Change Detail > Urgency	The urgency indicates how pressing the change is for the organization. The urgency and the impact are used to calculate the priority. This field functions similarly to the same field for interaction, incident, and problem tickets. For additional information, see User Interaction Management form details on page 44. This is a required field.
Change Detail > Priority	This is a system-generated field using the urgency and impact of the change. This field functions similarly to the same field for interaction, incident, and problem tickets. For additional information, see User Interaction Management form details on page 44.

Table 13-1 Change Management field descriptions (cont'd)

Label	Description
Change Detail > Risk Assessment	Specifies a code that indicates the risk incurred with the implementation of the change. This field becomes required in the Change Assessment and Planning phase. These risk assessments are available out-of-box: • 0 - No Risk • 1 - Low Risk • 2 - Some Risk • 3 - Moderate Risk • 4 - High Risk • 5 - Very High Risk After a user selects this field, the change may require additional approvals based on the risk. The approval is based on the risk number in the assessment approval record
Change Detail > Requested End Date	The system pre-populates this field if the change request is created from an interaction escalation. This is the date the change initiator requests the implementation of the change. This is a required field if not prepopulated.
Change Detail > Alert Stage	This is a system-generated field that lists the current Alert Stage of this request. Change Management updates this field automatically when processing alerts against this change. Do not update it manually. The alerts are processed against a change by using the Phase definition. This field is not active in an out-of-box system and must be manually enabled.
Change Detail > Planned Start	This field specifies the date and time that the work to implement the change should start. This field becomes required in the Change Assessment and Planning phase.
Change Detail > Planned End	This field specifies the date and time that the work to implement the change should end. This field becomes required in the Change Assessment and Planning phase.
Change Detail > Scheduled Downtime Start	The date and time when the change is scheduled to begin. Scheduled downtime only needs to be filled when the service is down, while implementing the change.
Change Detail > Scheduled Downtime End	The date and time when the change is scheduled to end. Scheduled downtime only needs to be filled when the service is down, while implementing the change.
Change Detail > Configuration Item(s) Down	If selected (set to true), indicates that the Configuration Items (CIs) are currently not operational and the downtime is scheduled. The fields Scheduled Downtime Start and Scheduled Downtime End are used along with the field Configuration Item(s) Down to indicate the scheduled time to bring the CI down. These fields are never required and should only be populated if you plan to bring down the CIs as part of the change. The interval selected applies to all the CIs of the change and cannot be specified by individual CI. When the change is closed, you may get the form confirming the outage times, and when you actually close the change, the CIs will be set as Up in Configuration Management.
Ex. Project Ref.	This field references an external project number.
Associated CI > Associated CI	This field provides the same data as the Affected CI field.
Associated CI > Field name	Displays the field name for the affected CI.
Associated CI > Completed/Cancelled CMDB Modifications	The data in this section is used by the UCMDB integration whenever there are past changes to the values registered for the CI.

Table 13-1 Change Management field descriptions (cont'd)

Label	Description
Affected Services **>** Affected Services	This notebook tab provides a list of affected services. When a configuration item for an incident is added or updated, a schedule record is created that runs a routine to update the list of affected services.
Approvals **>** Current Approvals **>**	This notebook tab provides an overview of the current approvals related to any changes for the CI as well as important information such as approval status, approvers This includes a list of groups or operators who must acknowledge or accept the risk, cost, and so on associated with the implementation of a Change request or task. Approvals give controlling authorities the ability to stop work and to control when certain work activities can proceed. The data displayed includes the following information: • Approval Type • Approval Status • # Approved • # Denied • # Pending
Approvals **>** Approval Log **>**	This notebook tab provides an overview of past approvals related to the changes for the CI as well as important information such as approval status and approvers. The data displayed includes the following information: • Action • Approver/Operator • By • Date/Time • Phase
Approvals **>** Pending Reviews **>** Reviewers	The name(s) of the groups or operator IDs that should review the change for the CI after it has been approved.
Plan **>** Plan	This tab provides space to give an assessment of the change, often generated by the Change Analyst, that the Change Coordinator uses to assess the impact of the change to services.
Task **>**	Whenever a change is in a phase where the user can generate tasks, Service Manager allows user a quick view of some of the most important fields in the task from the Task tab. The data displayed includes the following information: • Task No • Status • Approval Status • Assigned To • Description • Category
Backout Method	Provides a detailed method for backing out the change if there is a problem implementing the change. This is a required entry for an changes in the Unplanned Change category. It is also required in the Discovery Back Out phase and for the Release Management category in order to close the Release plan and design phase.

14 Configuration Management Overview

The HP Service Manager Configuration Management application, referred to as Configuration Management throughout this chapter, supports the Configuration Management process. It enables you to define and control the components of services and infrastructure, and to maintain accurate configuration information about the historical, planned, and current state of services and infrastructure.

Configuration Management ensures that you identify, baseline, and maintain selected components of a complete IT service, system, or product as Configuration Items and that you control changes to them by requiring formal approvals. Configuration Management also ensures that you control releases into your business environments.

This section describes how Configuration Management implements the best practice guidelines for the Configuration Management processes.

Topics in this section include:

Configuration Management within the ITIL framework

Configuration Management is addressed in ITIL's *Service Transition* publication. The document describes Configuration Management as the process responsible for managing services and assets to support the other Service Management processes.

Configuration Management is planned and implemented in conjunction with Change Management and Release Management to ensure that the service provider can manage its IT assets and configurations effectively. Configuration Management enables enterprises to efficiently identify, control, maintain, and verify the versions of CIs that exist in their infrastructure. Planning is an important part of Configuration Management, because planning ahead enables you to understand the impact that an incident or change could have on your infrastructure.

Responsibility for implementing controls can be delegated, but accountability remains with the responsible manager. Those authorizing the change should provide the manager with information on the cost, risks, and impact of a proposed change and a list of resources required for its implementation.

Configuration Management defines and controls the components of services and infrastructure and maintains accurate configuration information about the historical, planned, and current state of services and infrastructure.

Effective Configuration Management provides the following benefits:

- Accommodates changes to and reuse of standards and best practices.
- Significantly reduces incident resolution time by using a central repository for critical infrastructure data that can be accessed by other applications.
- Includes configuration grouping and business relationships.
- Enables you to meet business and customer control objectives and requirements.
- Provides accurate configuration information to enable people to make decisions at the right time. For example, to authorize changes and releases or to resolve incidents and problems faster.
- Minimizes the number of quality and compliance issues caused by improper configuration of services and assets.
- Optimizes the use of service assets, IT configurations, capabilities, and resources.

Configuration Management application

The Configuration Management application identifies, defines, and tracks an organization's CIs by creating and managing records for those items. Other Service Manager applications can then access these records from a central repository. For example, when you create an incident ticket, you can access the hardware component details from Configuration Management and populate the new incident with that information. Access to Configuration Management significantly reduces the time spent to resolve the incident, as well as alerts you to other potential incidents due to component relationships and dependencies defined in the database.

Configuration Management assures you that releases into controlled environments and operational use are performed on the basis of formal approvals. Configuration Management also provides a configuration model of services, assets, and infrastructure by recording relationships between service assets and configuration items.

All CIs are defined in the device file, the foundation of Configuration Management. Each CI record can include contact, location, vendor, and outage history. Other Service Manager applications, such as Incident Management and Change Management, access Configuration Management to populate fields on forms through the use of link records.

Configuration Management enables you to do the following:

- Identify, control, record, report, audit, and verify service assets and CIs, including versions, baselines, constituent components, and their attributes and relationships.
- Account for, manage, and protect the integrity of service assets and CIs throughout the service lifecycle by ensuring that only authorized components are used and only authorized changes are made.

As new and updated services and systems are released and distributed, accurate configuration information must be available to support the planning and control of changes. Service Manager's out-of-box Configuration Management workflow tracks the IT assets and configurations that make up the infrastructure. These assets can be hardware, software, and associated documentation. The inter-relationships between these components are also monitored. Effective results integrate the service provider's configuration information processes and those of its customers and suppliers. All major assets and configurations must be accounted for and have a responsible manager who ensures that protection and control is maintained.

User profiles determine the access level within Configuration Management. Depending on your access level, you can do the following:

- Add, edit, and save CI records.
- Manage CIs using predefined views to find CIs quickly.
- View and modify software installation information.
- View the maintenance schedule for a CI.
- View and modify SLA information.
- Add CIs to a contract and manage existing contracts.

HP Universal Configuration Management Database

An integration between HP Universal CMDB (UCMDB) and HP Service Manager enables you to share information about the actual state of a configuration item (CI) between your UCMDB system and Service Manager. Any organization that wants to implement the best practices Configuration Management and Change Management ITIL processes can use this integration to verify that CIs actually have the attribute values the organization has agreed to support.

A UCMDB is optional. Service Manager 7.10 Change Management and Configuration Management will work without it.

Service Manager allows you to programmatically define what actions you want to take whenever a CI's actual state does not match the expected state as defined in the CI record. For example, you can use this integration to automate the creation of Service Manager change or incident tickets to update or rollback CIs that have unexpected attribute values.

The integration offers several different ways for users to view CI actual state information:

- By default, the integration automatically updates the managed fields of Service Manager CI records as part of the regular UCMDB synchronization schedule. You can choose the option to configure the integration to automatically create change or incident tickets instead.
- You can view the current actual state of a CI by looking at the Actual State tab in the Service Manager CI record. For more information see Baselines on page 192, Managed state on page 193 and Actual state on page 193.
- You can use the Service Manager View in UCMDB option to log in to the UCMDB system and view the current CI attributes from UCMDB. A Service Manager user must have a valid UCMDB user name and password to log in to the UCMDB system.

You can specify CI relationships directly in Service Manager or define them in UCMDB and push them to Service Manager like any other asset, by using web services. You can also create UCMDB CI relationships from Service Manager CIs.

Baselines

Baselines are an optional feature of Configuration Management that allow you to define a set of attributes that all instances of a configuration item (CI) should have. A baseline is a template CI that defines the expected or authorized attributes of a CI. Typically, a baseline only describes the attributes that you expect CIs to share in common and does not include attributes that you expect to vary. For example, a baseline describing PCs might require that all PC CIs be assigned the same model number and operating system version but not the same owner or serial number. In this example, the model number and the operating system would be authorized attributes of the baseline, while the owner and the serial number would be individually-managed attributes.

Baseline records replace baseline configuration item groups from previous versions of Service Manager. The upgrade process converts existing baseline configuration item groups to query groups.

Baseline records are separate from the CI records they manage. You must first create a baseline record before you can associate it with one or more CIs. All baseline records must have a name, a list of authorized attributes, and a state. Baseline records can optionally have a version number, which administrators can configure from the Configuration Management environment record. A baseline record's status determines whether you can add or edit attributes, and whether you can associate CIs to the baseline. After you authorize a baseline record, its attributes are locked and you can only associate or remove CIs from the baseline.

It is up to a Configuration Management manager to determine whether a CI that is out of compliance with its baseline is acceptable or requires a change. Keep in mind that both the CI record and the baseline record describe the expected or managed state of a CI. A baseline record is intended to describe the expected state across many similar items. A CI record describes the expected state of an individual item.

There may be cases where it is acceptable for an individual CI to have a different managed state than other CIs in the same baseline. For example, you might have a baseline requiring that all application servers have 8 GB of RAM. However, you may also want one of your application servers, the Web server, to have 16 GB of RAM. You may want to authorize this exception to the baseline rather than creating a new baseline record to describe just one CI.

Baselines only check for compliance against the managed state of the CI. The actual state of the CI is irrelevant to a baseline compliance check. Continuing the example above, the Web server CI record might list 16 GB of RAM as the managed state. This makes it out of compliance with the baseline that requires all application servers to have 8 GB of RAM. If a discovery process later reveals that the Web server actually only has 12 GB of RAM, this might cause Service Manager to open an unplanned change, but it will not cause a new violation of the baseline. Only differences between the CI's managed state (16 GB of RAM) and the baseline (8 GB of RAM) matter.

Baseline notebook tab

Each CI record has a baseline notebook tab that lists details about the baseline, if any, that is currently managing the CI. The baseline notebook tab lists the name of the managing baseline, its version, and a list of the attribute names and attribute values the baseline expects. If the CI has a value other than the baseline value, Service Manager displays a warning message that the Configuration Item is out of compliance with Baseline.

Managed state

In Service Manager, the managed state is the subset of CI attributes that have been defined as critical enough to be closely managed by a formal change process and have been approved by that process. You may add managed state information for a CI in several ways:

- Automatically add CI attributes from an integration to HP Universal CMDB
- Automatically add CI attributes from an integration to Connect-It and HP Universal CMDB
- Manually add CI attributes

After you add the managed state information to a CI, any changes to the CI attributes must go through a Change Management process.

Service Manager owns the managed state of a CI and acts as the definitive source of what the CI attributes should be. The actual state of the CI may differ from the managed state and may trigger actions in Service Manager such as an out of compliance with baseline warning message or the opening of an unplanned change.

Managed State notebook tab

The Managed State notebook tab uses sub-tabs to display data about each CI. There are three sub-tabs for this purpose, The Network sub-tab and the Additional sub-tab are used for all CI types. The third sub-tab depends upon the CI and CI type selected. For example, the Adobe Reader is an application CI type and therefore includes the Application sub-tab on the Managed State tab.

Actual state

The actual state of a CI is the current list of CI attributes. By default, Service Manager only stores and displays the expected or managed state of CIs. Service Manager can only receive actual state information if you set up an integration to HP Universal CMDB. Service Manager uses the actual state to determine if a CI is in compliance with its managed state. Service Manager compares the managed attribute values listed in the CI record to the attributes values listed in HP Universal CMDB. If any of the managed attribute values differ from the managed state, Service Manager takes action as defined in the Discovery Event Manager (DEM) settings. By default, Service Manager opens an unplanned change whenever the actual state of a CI attribute differs from the managed state.

Actual State notebook tab

The Actual State notebook tab displays the list of CI attributes passed from an HP Universal CMDB integration. The list of CI attributes varies from CI to CI and may not match your list of managed attributes. That is, the Actual State notebook tab displays all the CI attributes it receives from the HP Universal CMDB integration whether they are managed fields in Service Manager or not.

To view the actual state of the CI, you must first create an integration to a HP Universal CMDB server. The HP Universal CMDB server periodically discovers the actual state of CIs and records the actual state in the Configuration Management database. Service Manager accesses the actual state information by using a Web services connection. Service Manager sends the CI ID to the HP Universal CMDB server and receives a full list of the attributes for that CI. Service Manager displays the CI attributes on the Actual State notebook tab of the Configuration Management form.

If a Service Manager CI does not have a matching CI in the HP Universal CMDB server, then Service Manager does not display the Actual State notebook tab. For example, you may track office furnishing CIs in Service Manager that cannot be discovered and tracked in the HP Universal CMDB.

CI relationships

Service Manager tracks upstream and downstream relationships between CIs. A relationship between CIs means that there is some dependency between CIs. If an upstream CI has an interruption of service, Service Manager assumes that all CIs with a downstream relationship to the affected CI also have an interruption of service. For example, if a network router has an interruption of service, then all servers and PCs that connect to that router also have an interruption of service.

Any given CI typically has one upstream relationship and one or more downstream relationships. CIs can have logical or physical relationships based on the logical name of the configuration item. CI relationships are independent of baseline, actual or managed states.

CI Relationship tab (CI visualization)

Each CI record has a notebook tab that graphically displays relationships between CIs and the current state of each item in the configuration. (UCMDB has a similar relationship diagram.) Service Manager gathers information from all available applications to determine the current state of a CI. You can view, add, or update relationships using the graphical interface. Service Manager uses smart indicators to tell you if there are any current issues, related records, or breeches to availability SLAs for the CI.

Configuration Management process overview

The Configuration Management process ensures that selected components of a complete IT service, system, or product (the Configuration Item) are identified, baselined, and maintained and that changes to them are controlled. It provides a Configuration model of the services, assets, and infrastructure by recording the relationships between service assets and Configuration Items. It also ensures that releases into controlled environments and operational use are completed on the basis of formal approvals. It provides a configuration model of the services, assets, and infrastructure by recording the relationships between service assets and Configuration Items (CIs).

Configuration Management may cover non-IT assets, work products used to develop the services, and Configuration Items required to support the services that are not formally classified as assets. Any component that requires management to deliver an IT Service is considered part of the scope of Configuration Management.

The asset management portion of this process manages service assets across the whole service life cycle, from acquisition to disposal. It also provides a complete inventory of assets and the associated owners responsible for their control.

The Configuration Management portion of this process maintains information about any CI required to deliver an IT service, including its relationships. This information is managed throughout the life cycle of the CI. The objective of Configuration Management is to define and control the components of an IT service and its infrastructure, and to maintain accurate configuration information.

The Configuration Management process manages service assets to support other Service Management processes. Effective Configuration Management facilitates greater system availability, minimizes production issues, and resolves issues more efficiently.

The Configuration Management process ensures that selected components of a complete IT service, system, or product (the Configuration Item) are identified, baselined, and maintained and that changes to them are controlled. It also ensures that releases into controlled environments and operational use are completed on the basis of formal approvals.

Configuration Management comprises five basic activities. The Configuration Management process encompasses all of these activities and ensures that assets are tracked and monitored effectively. The basic activities within the scope of Configuration Management are:

- Configuration Management Planning (process ST 3.1) on page 201 — includes the activities that enable you to plan the function, scope, and objectives of Configuration Management for your organization.
- Configuration Identification (process ST 3.2) on page 204 — includes the activities that enable you to identify and label all of your company's existing IT components. The information you track includes asset identification, contact, asset network relationship, and model or version data. Enter this information into the database.
- *Inventory maintenance*
  - Configuration Control (process ST 3.3) on page 207 — includes the activities that enable you to ensure that all information regarding your IT components is kept up to date and accurate. Components can be added, modified, or removed only through controlling documentation, such as an approved Request for Change (RFC).
  - Master data management (process ST 3.6) on page 217 — includes the activities that enable you to reconcile master reference data managed in other administrations.
- Configuration Status Accounting and Reporting (process ST 3.4) on page 210 — includes the activities that enable you to run reports of the current and historical data that is concerned with each IT component throughout its life cycle. Status accounting makes changes to components trackable.
- Configuration Verification and Audit (process ST 3.5) on page 213 — includes the activities that enable you to check and verify physical existence of IT components and ensure that they are correctly recorded in the database.

A general overview of the Configuration Management processes and workflows is depicted in Figure 14-1, below. They are described in detail in Chapter 15, Configuration Management Workflows.

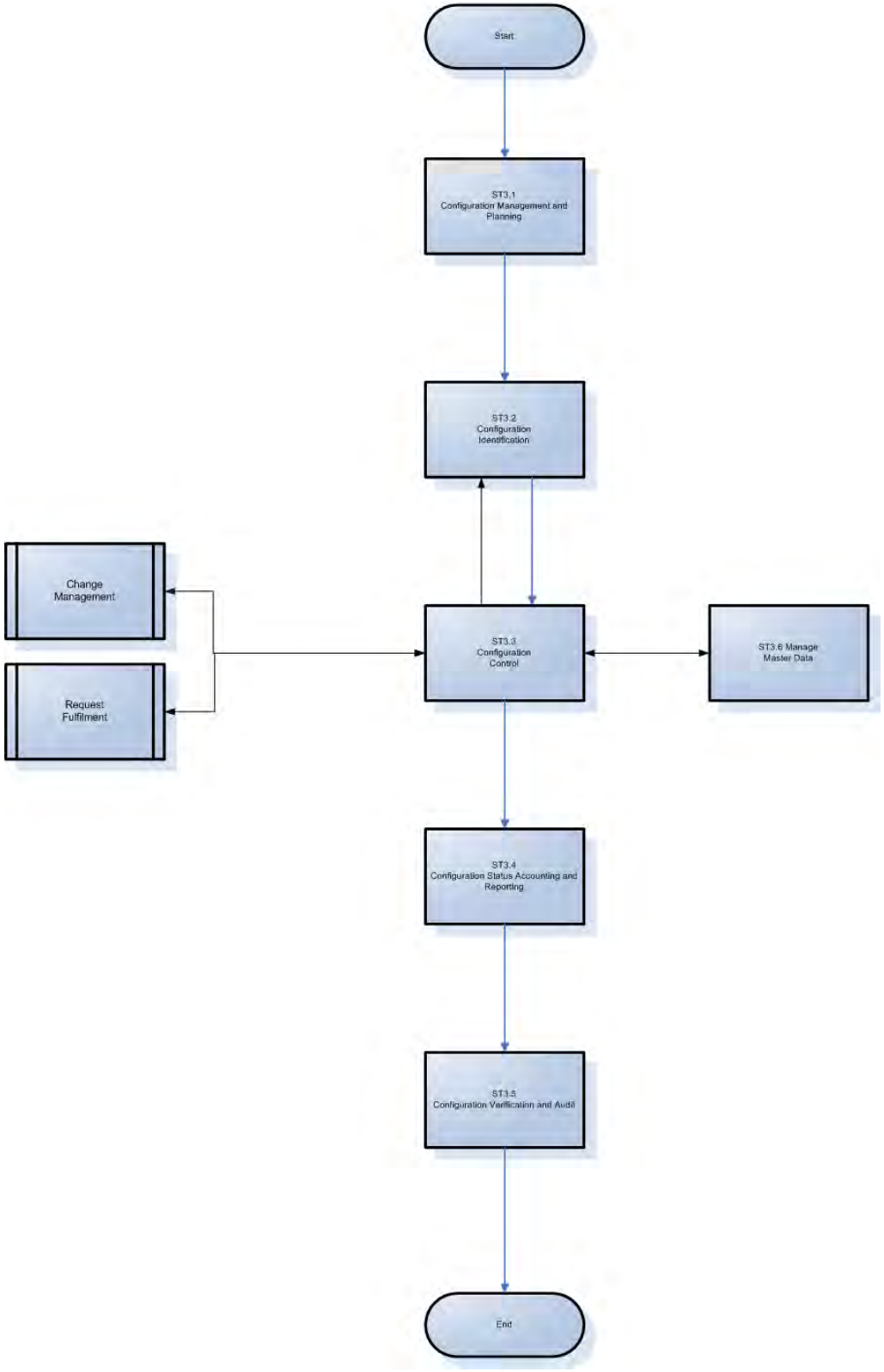

Figure 14-1 Configuration Management process diagram

Configuration Management user roles

Table 14-1 describes the responsibilities of the Configuration Management user roles.

Table 14-1 Configuration Management user roles

Role	Responsibilities
Configuration Administrator	• Reviews proposed updates to the Configuration Management system (CMS) • Evaluates the pre-modification and post-modification configuration states. • Verifies that CI information is correct and complete and contains a description of attributes to be modified. • Verifies that proposed modifications comply with Configuration Management policies. • Verifies that Configuration details are updated in the Configuration Management database.
Configuration Auditor	• Reviews and validates CMS updates and creates exception reports, if needed. • Conducts configuration audits and performs appropriate actions, if an unregistered component is detected or if a component is missing. • Ensures that information in Configuration Management is correct and that all CIs are accurately and completely recorded.
Configuration Manager	• Manages the Configuration Management plan and policies. • Evaluates any task that requests a change to the CMS data model before the manager releases the task for implementation. For example, the introduction of a new CI into the IT infrastructure would require a request for change and a review of that request prior to implementation of the change. • Verifies that there is no existing CI type that meets the needs of the change and that the proposed data model change does not conflict with other parts of the model.
CMS/Tools Administrator	Configures the data model, policies, and CI types in Service Manager.

Input and output for Configuration Management

Configuration activities can be triggered and resolved in several ways. Table 14-2 outlines the inputs and outputs for the Configuration Management process.

Table 14-2 Input and output for Configuration Management

Input to Configuration Management	Output from Configuration Management
• Changes required in the Configuration Management System (CMS) • Tasks initiated from changes or service requests to create or modify Configurations Items (CIs) and relationships	• Configuration Management plan • Configuration Management policies • Configuration Management data model (defining CI types and attributes) • Configuration reports (for example, overview of CIs, subscriptions, license reports, stock reports, or configuration utilization reports) — Configuration audit report • Incidents reported due to discrepancies or unauthorized changes detected • Creation and modification of CIs and configuration data

Key performance indicators for Configuration Management

The Key Performance Indicators (KPIs) in Table 14-3 are useful for evaluating your Configuration Management processes. To visualize trend information, it is useful to graph KPI data periodically. Note that some KPIs cannot be reported by using only the data from Service Manager.

Table 14-3 Key Performance Indicators for Configuration Management

Title	Description
% of CIs related to Services	Number of CIs that are related to one or more IT services as a percentage of the total number of registered CIs that can be related to IT services, in a given time period.
% of CIs related to other CIs	Number of CIs related to one or more other CIs as a percentage of the total number of registered CIs that can be related to other CIs, in a given time period.
% of inaccurate CIs	Number of CIs in the CMS that are registered with inaccurate information as a percentage of the total number of registered CIs, in a given time period.

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included below.

ITIL V3 key performance indicators

The following are ITIL V3 KPIs for Configuration Management:

- Percentage improvement in maintenance scheduling over the life of an asset
- Degree of alignment between provided maintenance and business support
- Assets identified as the cause of service failures
- Improved speed for Incident Management to identify faulty CIs and restore service
- Impact of incidents and errors affecting particular CI types, for example, from particular suppliers or development groups, for use in improving the IT service
- Percentage reuse and redistribution of under-utilized resources and assets
- Degree of alignment of insurance premiums with business needs
- Ratio of used licenses against paid for licenses (should be close to 100%)
- Average cost per user for licenses (that is, more effective charging options achieved)
- Achieved accuracy in budgets and charges for the assets utilized by each customer or business unit
- Percentage reduction in business impact of outages and incidents caused by Configuration Management
- Improved audit compliance

COBIT 4.1 key performance indicators

The following are the COBIT 4.1 KPIs for Configuration Management:

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between the configuration repository and actual asset configurations
- Percent of licenses purchased and not accounted for in the repository
- Average lag time period between identifying a discrepancy and rectifying it
- Number of discrepancies relating to incomplete or missing configuration information
- Percent of configuration items meeting specified service levels for performance, security, and availability

RACI matrix for Configuration Management

A Responsible, Accountable, Consulted, and Informed (RACI) diagram or RACI matrix is used to describe the roles and responsibilities of various teams or people in delivering a project or operating a process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. The RACI matrix for Configuration Management is shown in Table 14-4.

Table 14-4 RACI matrix for Configuration Management

Process ID	Activity	Configuration Manager	CMS/Tools Administrator	Configuration Administrator	Configuration Auditor	Change Coordinator
ST 3.1	Configuration Management Planning	A/R	R			
ST 3.2	Configuration Identification	A/C		R		C/I
ST 3.3	Configuration Control	A/C		R		C/I
ST 3.4	Configuration Status Accounting and Reporting	A/I		R	R	
ST 3.5	Configuration Verification and Audit	A/C		R	R	
ST 3.6	Manage Master Data	A		R		

15 Configuration Management Workflows

The Configuration Management process manages service assets to support other Service Management processes. Effective Configuration Management facilitates greater system availability, minimizes production issues, and resolves issues more efficiently.

The Configuration Management process consists of the following processes, which are included in this chapter:

Configuration Management Planning (process ST 3.1)

Infrastructure and services should have an up-to-date Configuration Management plan, which can stand alone or form part of other planning documents. The Configuration Management plan should include or describe the following:

- Scope, objectives, policies, standards, roles, and responsibilities
- Configuration Management processes to provide the following services:
  - Define the Configuration Items that comprise related service(s) and infrastructure
  - Control changes to configurations
  - Record and report the status of Configuration Items
  - Verify the completeness and correctness of Configuration Items according to the requirements for accountability, traceability, and auditability
- Configuration Control (access, protection, version, build, and release controls)
- Interface control process for identifying, recording, and managing CIs and information at the common boundary of two or more organizations (for example, system interfaces and releases)
- Planning and establishing the resources to bring assets and configurations under control and maintain the Configuration Management system (for example, training)
- Management of suppliers and subcontractors performing Configuration Management

Details for this process can be seen in the following figure and table.

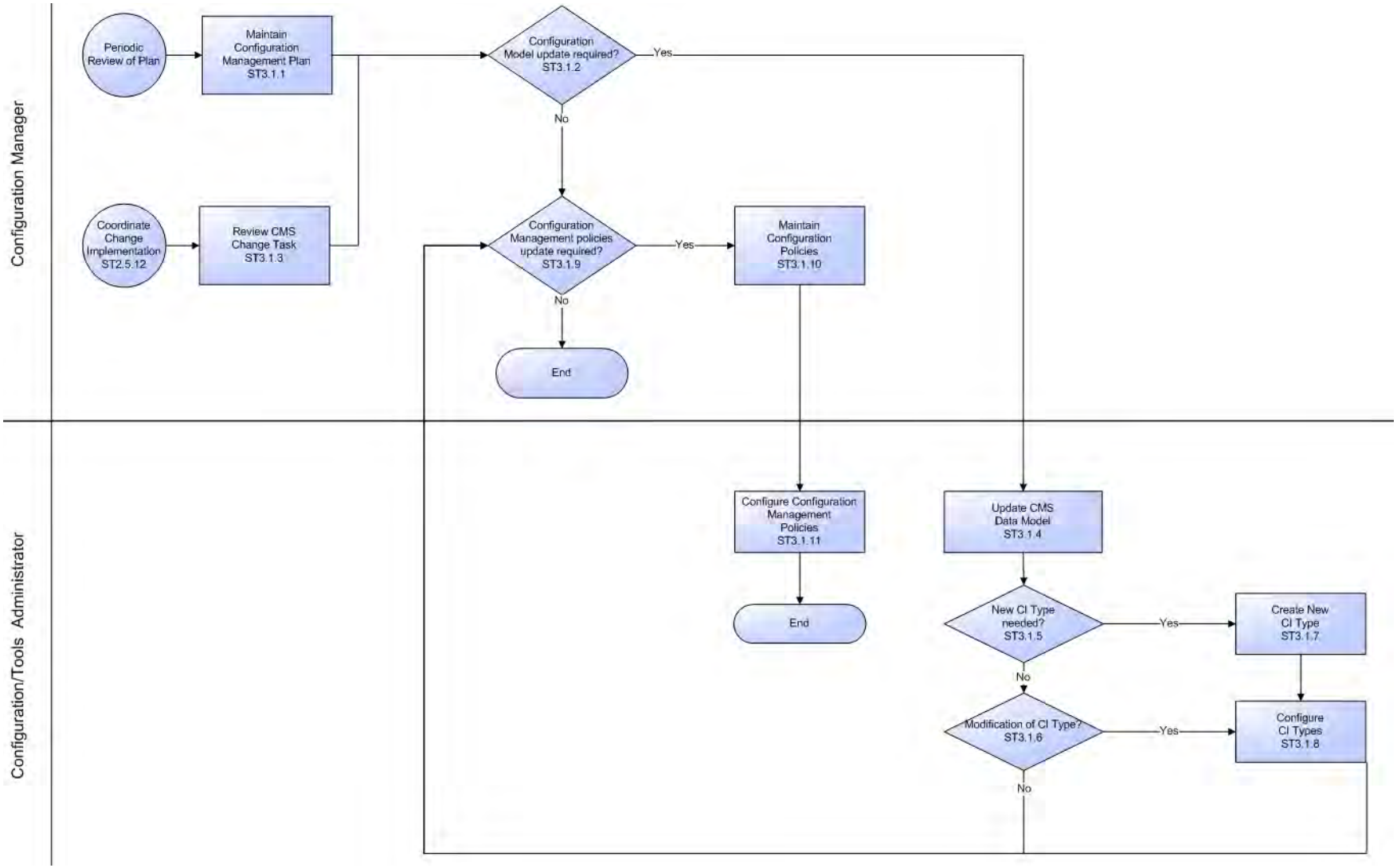

Figure 15-1 Configuration Management Planning workflow

Table 15-1 Configuration Management Planning process

Process ID	Procedure or Decision	Description	Role
ST 3.1.1	Maintain Configuration Management plan	The Configuration Manager maintains the Configuration Management policies, objectives, scope, and principles. Periodically, this plan is reviewed to determine improvements. The Configuration Management plan (ACM plan) also defines the scope and level of detail of Configuration Item (CI) data to be maintained in the CMS. A Configuration Management plan provides the guidelines for documenting and modeling IT services in the CMS (identification of CIs).	Configuration Manager
ST 3.1.2	Configuration model update required?	Determine whether the Configuration model should be updated. If yes, go to ST 3.1.4. If no, go to ST 3.1.9.	Configuration Manager
ST 3.1.3	Review CMS change task	The Configuration Manager receives a task from Configuration Management to update the CMS data model (for example, when a new type of CI is introduced in the IT infrastructure as a result of a release).	Configuration Manager
ST 3.1.4	Update CMS data model	The data model defines the structure and information model of the CMS. This includes: • Model of IT services (breakdown of services into service components) • CI relationships types • Definition of CI types • Definition of CI attributes • Identification of data sources (such as HR-system or ERP) The Configuration Manager determines the type of modification that is required for the CMS model.	CMS/Tools Administrator
ST 3.1.5	New CI type needed?	If a new CI type is needed, go to ST 3.1.7. If not, continue with ST 3.1.6.	CMS/Tools Administrator
ST 3.1.6	Modification of CI type required?	If a modification of the CI type is required, go to ST 3.1.8. If not, continue with ST 3.1.9.	CMS/Tools Administrator
ST 3.1.7	Create new CI type	The CMS/Tools Administrator adds a new CI type (device type). This includes the definition of CI attributes and screen design.	CMS/Tools Administrator
ST 3.1.8	Configure CI types	Create or modify the definition of the CI type. This includes: • CI subtypes • Attribute definitions • Screen design • CI relationships types • Naming conventions • Business rules on required fields	CMS/Tools Administrator

Table 15-1 Configuration Management Planning process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 3.1.9	Configuration Management policies update required?	The Configuration Administrator determines whether the Configuration Management policies must be updated (to reflect the SCAM plan). If so, go to ST 3.1.10.	Configuration Manager
ST 3.1.10	Maintain Configuration Management policies	The Configuration Manager maintains the Configuration Management policies. Policies may be applicable for specific asset types (or CI Types) or services. Policies may include business rules and requirements for specific information to be maintained in the CMS (for example, for compliance purposes or to monitor contracts). Policies determine how often a configuration audit is required. Policies also designate which data in a CI may be updated by inventory tools, as well as what actions must be performed if unauthorized software is detected. Other items covered by policies and business rules include: • Naming conventions • Labeling rules • Asset capitalization rules (for example, to set the depreciation start date) • Procedures for lost or stolen items	Configuration Manager
ST 3.1.11	Configure Configuration Management policies	Configuration Management policies and requirements are translated into tool settings (for example, required fields, schedule for automated inventory and discovery, and reconciliation rules).	CMS/Tools Administrator

Configuration Identification (process ST 3.2)

In the Configuration Identification process, the Configuration Administrator selects Configuration Items (CIs), records their identifying characteristics, and assigns unique identifiers to the selected items. This process helps to ensure efficient data storage and retrieval.

Configuration Identification process is enables you to do the following:

- Identify and register CIs
- Assign unique labels
- Record relationship information

Configuration Identification is responsible for collecting information about CIs and their relationships, and for loading this information into Configuration Management. Configuration Identification is also responsible for labeling the CIs, which enables the corresponding configuration records to be found.

Details for this process can be seen in the following figure and table.

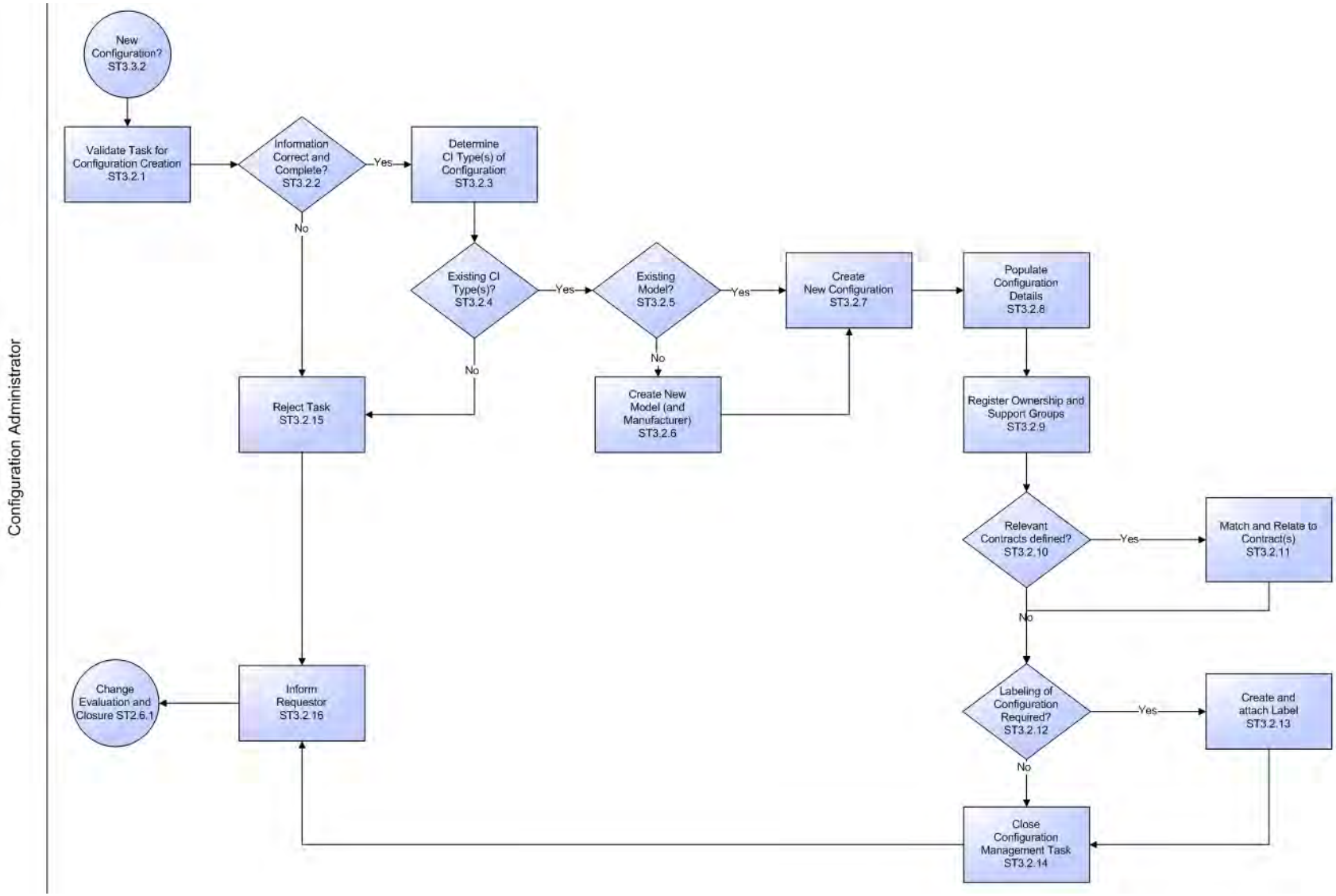

Figure 15-2 Configuration Identification workflow

Table 15-2 Configuration Identification process

Process ID	Procedure or Decision	Description	Role
ST 3.2.1	Validate task for configuration creation	The Configuration Administrator reviews the task to verify that all required information to create a new configuration is complete and correct. Configuration describes a group of CIs that work together to deliver an IT Service, or a recognizable part of an IT Service. The term configuration can also refer to the parameter settings for one or more CIs.	Configuration Administrator
ST 3.2.2	Information correct and complete?	If the information is correct and complete, continue with ST 3.2.3. If not, go to ST 3.2.15 (reject task).	Configuration Administrator
ST 3.2.3	Determine CI type(s) of configuration	Determine the CI type(s) needed to register the CIs. A CI type is used as a template to document the CI, including, attributes and required fields.	Configuration Administrator
ST 3.2.4	Existing CI type(s)?	A CI can only be registered if the CI type is known and a Configuration Management policy is available for these types. Existing types must match the attributes that need to be managed and allow designation of a person who is responsible for maintaining the CI. CIs of a registered type can be used as templates for new CIs. If there are existing CI types, continue with ST 3.2.5. If not, go to ST 3.2.15 (reject task).	Configuration Administrator
ST 3.2.5	Existing model?	Verify that the models (the product definition from the manufacturer or supplier) for the configuration exist. A model refers to the product catalog defining the approved and certified list of components, which can be deployed within the IT environment. If there are no models, go to ST 3.2.6 to create a new model. If yes, continue with ST 3.2.7 (create new configuration).	Configuration Administrator
ST 3.2.6	Create new model and manufacturer	Create a new model. The model contains information, such as the Model name, Manufacturer, and ID of component discovered by monitoring tools (for example, software component name).	Configuration Administrator
ST 3.2.7	Create new configuration	Create the CIs part of the configuration. One or more CIs can be created. Select the CI type (template). Select the model.	Configuration Administrator
ST 3.2.8	Populate configuration details	Enter the required CI attributes, according to the Configuration Management policies. Capture relationships and dependencies between the CIs. Depending upon the CI type and business rules, examples of details include: • Serial number location (for example, on stock) • Purchase order number • Receipt date warranty conditions and warranty end date • CI specific attributes	Configuration Administrator

Table 15-2 Configuration Identification process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 3.2.9	Register ownership and support groups	All CIs must be assigned to an owner (that is, a reference to an organizational entity such as a cost center) and an administrator (the group responsible for managing the CI during its life cycle). Activities include: • Assign owner • Assign Configuration Administrator (group) • Assign support group for incident assignment (for example, if needed for automated assignment in case of events detected on the device)	Configuration Administrator
ST 3.2.10	Relevant contracts defined?	Determine related contracts for the components, such as: • Maintenance or support contracts • Financial contracts (for example, lease or rental) • License contract or service contracts (for example, SLA, UC, and OLA) If no contracts are relevant for this Configuration, go to ST 3.2.12. If yes, continue with ST 3.2.11 to link the items to the contract.	Configuration Administrator
ST 3.2.11	Match and relate to contract(s)	Link the CIs to one or more contracts. Capture the inclusion date of the CI to the contract. If needed, inform the Contract Manager of the new items attached to the contract.	Configuration Administrator
ST 3.2.12	Labeling of configuration required?	Determine whether CIs need to be labeled according to the Configuration Management policies. If not, go to ST 3.2.14. If yes, continue with ST 3.2.13.	Configuration Administrator
ST 3.2.13	Create and attach label	Create and print a label. Physically attach the label to the CI.	Configuration Administrator
ST 3.2.14	Close Configuration Management task	After completion, the task can be closed. Update closure code.	Configuration Administrator
ST 3.2.15	Reject task	If the task cannot be completed, reject the task. Update the task with reasons and details of any issues found.	Configuration Administrator
ST 3.2.16	Inform requester	Inform the requester of the completion or rejection. If needed, provide additional information, such as the reason and advice on appropriate next steps.	Configuration Administrator

Configuration Control (process ST 3.3)

In the Configuration Control process, the Configuration Administrator reviews the Configuration Management task for updating the Configuration Management system (CMS) and evaluates the configuration in its premodification and postmodification state. The Configuration Administrator verifies the information is correct and complete, and contains a description of attributes to be modified; the proposed modifications comply with Configuration Management policies; and that the configuration details are updated in the Configuration Management database.

Details for this process can be seen in the following figure and table.

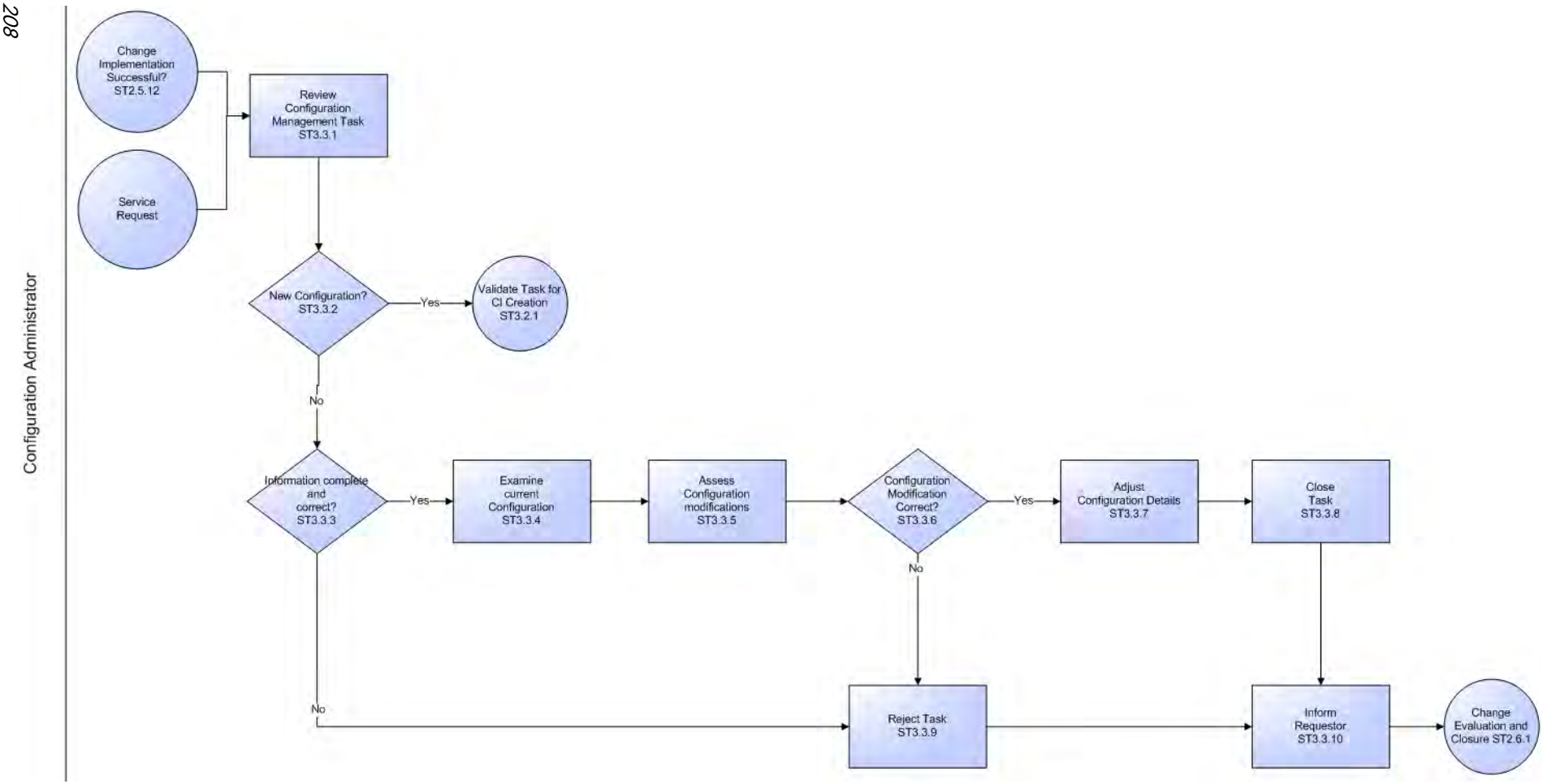

Figure 15-3 Configuration Control workflow

Table 15-3 Configuration Control process

Process ID	Procedure or Decision	Description	Role
ST 3.3.1	Review Configuration Management task	The Configuration Administrator reviews the task for updating the Configuration Management System (CMS).	Configuration Administrator
ST 3.3.2	New configuration?	If the task refers to the creation of one or more new CIs, go to ST 3.2.1 and follow the procedure to validate a task for CI creation. If the task is related to the modification of an existing CI, continue with ST 3.3.3.	Configuration Administrator
ST 3.3.3	Information complete and correct?	Verify that all information to update the CIs is available and correct. The task should refer to at least one CI that must be updated. The task contains a description of the attributes to be modified. If not all information is complete and correct, go to ST 3.3.9 (reject task). If yes, continue with ST 3.3.4.	Configuration Administrator
ST 3.3.4	Examine current configuration	Before the modification is implemented, the current state of the CIs must be reviewed to verify the expected starting point for the change.	Configuration Administrator
ST 3.3.5	Assess configuration modifications	Verify the proposed modifications to ensure that these are correct and complete (that is, according to Configuration Management policies).	Configuration Administrator
ST 3.3.6	Configuration modification correct?	If the configuration modification is correct, continue with ST 3.3.7. If not, go to ST 3.3.9 (reject task).	Configuration Administrator
ST 3.3.7	Adjust configuration details	Modify the configuration details in the Configuration Management database. Configuration modifications can include: • Status (items transferred from test to production or to retirement) • Location (moves) • Relationships and dependencies • Installation of software on the item • Transfer of ownership • Assign contract to a CI	Configuration Administrator
ST 3.3.8	Close task	After completion of the configuration updates, the task can be closed.	Configuration Administrator
ST 3.3.9	Reject task	If the configuration update cannot be completed, the task is rejected. A reason and recommended actions must be provided.	Configuration Administrator
ST 3.3.10	Inform requester	The requester is informed of the closure or rejection of the task. Continue with ST 2.6.1 (Change Review and closure).	Configuration Administrator

Configuration Status Accounting and Reporting (process ST 3.4)

Configuration Status Accounting and Reporting ensures that all configuration data and documentation are recorded as each CI progresses through its life cycle from test to production to retirement. Configuration information should be kept current and made available for planning, decision making, and managing changes to the defined configurations.

Configuration Status Accounting and Reporting keeps track of the following CI status changes:

- New items received (as evidenced by a goods receipt procedure or from development)
- Installation of items
- Transition from test to production
- System down (based upon events)
- Retired or disposed items
- Lost or stolen items
- Unauthorized CIs and Version changes of CIs

Current and accurate configuration records should be maintained to reflect changes in the status, location, and versions of CIs. The history of each CI must be maintained. Changes to CIs are tracked through various states, such as ordered, received, in acceptance test, live, under change, withdrawn, or disposed.

Where required, configuration information should be accessible to users, customers, suppliers, and partners to assist them in their planning and decision making. For example, an external service provider may make configuration information accessible to the customer and other parties to support the other service management processes in an end-to-end service. Archiving procedures should be defined for data related to retired or disposed CIs.

Configuration Management reports should be available to all relevant parties. The reports should cover the identification and status of the CIs, including their versions and associated documentation. A large set of different reports are needed for the different stakeholders (for example, audit reports, software compliance reports, and charge back reports).

Details for this process can be seen in the following figure and table.

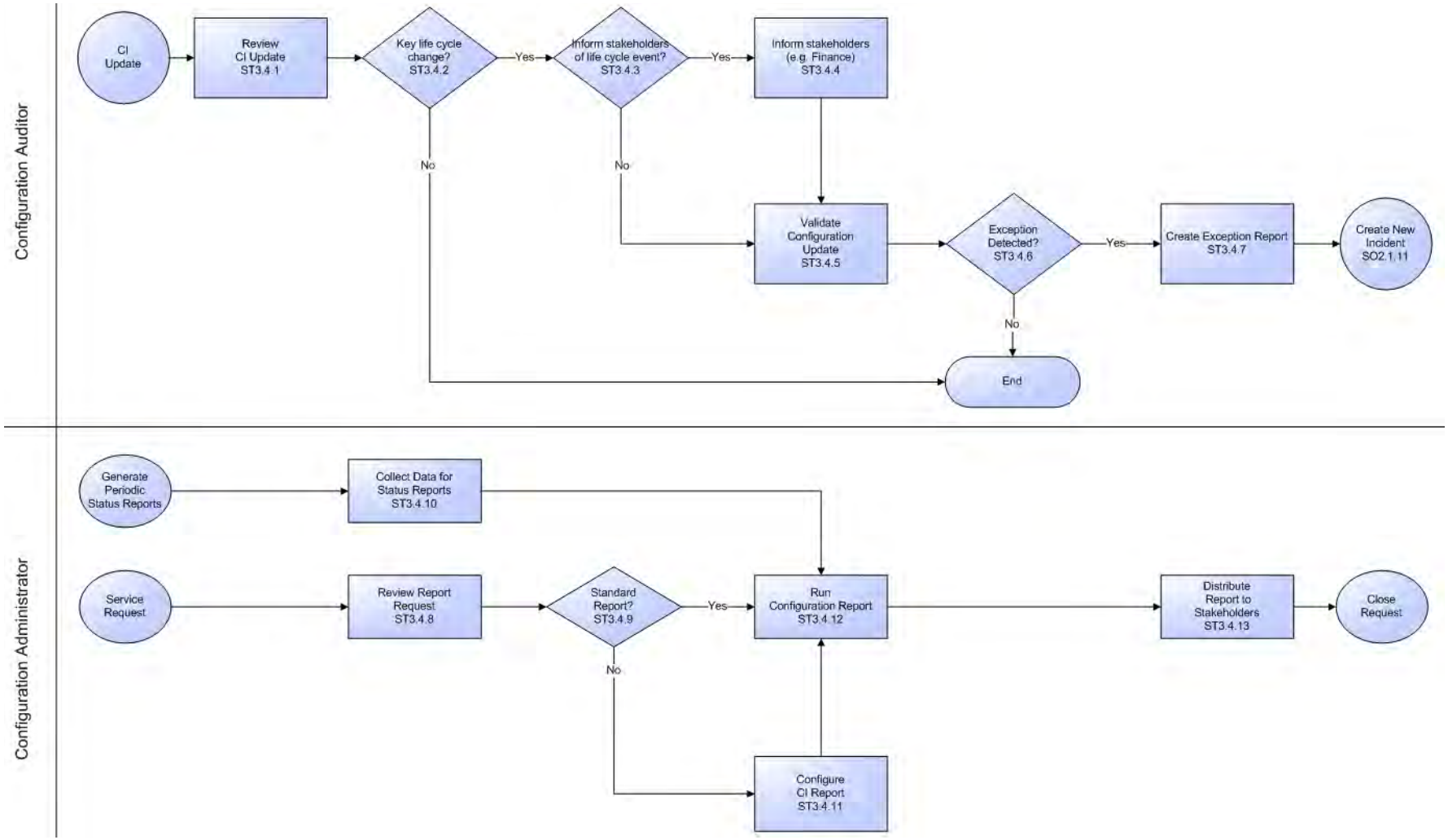

Figure 15-4 Configuration Status Accounting and Reporting workflow

Table 15-4 Configuration Status Accounting and Reporting process

Process ID	Procedure or Decision	Description	Role
ST 3.4.1	Review CI update	Modifications of key attributes of the CI are logged in the history log and verified. During Configuration Identification and control activities, configuration status records are created. These records enable key changes to be visible and traceable. CI attributes that can be logged include: • status (for example, system down) • version number • serial number • installation date • audit status (for example, missing or lost) • removed from a contract Critical CI changes are logged with entries for reason, date stamp, time stamp, and person recording the status change.	Configuration Auditor
ST 3.4.2	Key life cycle change?	Determine whether the modification must be reviewed or validated, based on the documented Configuration Management policies (and policies related to finance, procurement, Contract Management, and security).	Configuration Auditor
ST 3.4.3	Inform stakeholders of life cycle event?	Specific life cycle events must be reported to the stakeholders. These include: • Procurement • Finance (for example, by linking to the general ledger) • Contract Manager Verify that the event must be reported. If not, go to ST 3.4.5. If yes, continue with ST 3.4.4.	Configuration Auditor
ST 3.4.4	Inform stakeholders	Inform stakeholders of the event (for example, the Contract Manager when an asset is included in the contract, or procurement when an item is received). Examples of events that should trigger stakeholder notification include: • Received and accepted items • Installation of the asset (for example, for depreciation start date) • Lost or stolen item • Retirement or disposal of an item (for finance)	Configuration Auditor
ST 3.4.5	Validate configuration update	Confirm that all relevant status data documented in the CI is complete and correct, according to Configuration Management policies derived from agreements, relevant legislation, and standards. Ensure that the status change or version update is a result of an authorized change.	Configuration Auditor
ST 3.4.6	Exception detected?	If the CI update or CI details are not correct or complete according to the Configuration policies, continue with SO3.4.7.	Configuration Auditor
ST 3.4.7	Create exception report	Create a new incident (see SO 2.1.11).	Configuration Auditor

Table 15-4 Configuration Status Accounting and Reporting process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 3.4.8	Review report request	The Configuration Administrator reviews the request for Configuration Management information.	Configuration Administrator
ST 3.4.9	Standard report?	Configuration Management has defined a number of standard reports (for example, overview of CIs in stock or by status). If this is a standard report, continue with ST 3.4.12. If not, go to ST 3.4.11.	Configuration Administrator
ST 3.4.10	Collect data for status reports	Periodically, Configuration Management procedures provide reports for the different stakeholders, such as financial asset managers, contract managers, or procurement.	Configuration Administrator
ST 3.4.11	Configure CI report	If a standard report does not exist, the Configuration Administrator creates a query to select the data to display from the CMS.	Configuration Administrator
ST 3.4.12	Run configuration report	The report or query is run against the database. The data is collected in a standard format.	Configuration Administrator
ST 3.4.13	Distribute report to stakeholders	Provide the requested data to the stakeholders. Close the request (if applicable).	Configuration Administrator

Configuration Verification and Audit (process ST 3.5)

Verification and auditing is responsible for ensuring that information in Configuration Management is accurate and that all Configuration Items (CIs) are identified and recorded in Configuration Management. The process can be conducted manually, or by using automated inventory and discovery tools.

Verification includes routine checks that are part of other processes (for example, verifying the serial number of a desktop PC when a user logs an incident). Audit is a periodic, formal check. You should verify and audit your configurations regularly to ensure proper functioning of the entire Configuration Management process, and for related IT service management processes.

The objective of verification and auditing for Configuration Management is to detect and manage all exceptions to configuration policies, processes, and procedures, including security and license use rights. The verification process ensures that configuration records are accurate and complete, and that any recorded changes are approved. Configuration audits help to maintain the integrity of the Configuration Management System (CMS).

Also included in the configuration and audit process is the periodic review of installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements.

Configuration Verification and Audit activities include:

- Make sure that baselines and standards match the actual components in the IT environment
- Verify that services and products are built and documented, according to documented requirements, standards, or contractual agreements
- Verify that the correct and authorized versions of any CI exists and is correctly identified and described
- Verify the physical existence of CIs (for example, in the organization, in the Definitive Media Library, or in stock)
- Check that release documentation and configuration administration are present before making a release

- Confirm that the current environment is as expected and documented in the CMS, and that any Change requests are resolved
- Check that configuration modifications are implemented through authorized changes
- Validate the existence of a SLA against each CI
- Verify that CI specifications are compliant with defined configuration policies and baselines
- Validate that all required documentation for each CI is available (for example, maintenance contracts, license records, or warranties)
- Check data quality for accuracy and completeness
- Initiate an incident ticket for discovered unauthorized changes

The following are examples of discrepancies:

- Unauthorized software installed
- Unauthorized access to resources and services (for example, access rights not reflected in subscriptions)
- Discrepancy of status or configuration details, as registered in the CMS, compared with the actual status.

Configuration Verification and Audit processes, both physical and functional, should be scheduled and a check performed to ensure that adequate processes and resources are in place. Benefits of this process include:

- Protection of the physical configurations and the intellectual capital of the organization
- Verification that the service provider is in control of its configurations, master copies, and licenses
- Confidence that configuration information is accurate, controlled, and visible
- Conformance of changes, releases, systems, and IT environments to contracted or specified requirements.
- Accuracy and completeness of configuration records

Configuration audits should be carried out regularly, before and after a major change (or release), after a disaster, and at random intervals. Deficiencies and nonconformities should be recorded, assessed and corrective action initiated, acted on, and reported back to the relevant parties and plan for improving the service. Unauthorized and unregistered items that are discovered during the audit should be investigated and corrective action taken to address possible issues with procedures and the behavior of personnel. All exceptions are logged and reported as incidents.

Details for this process can be seen in the following figure and table.

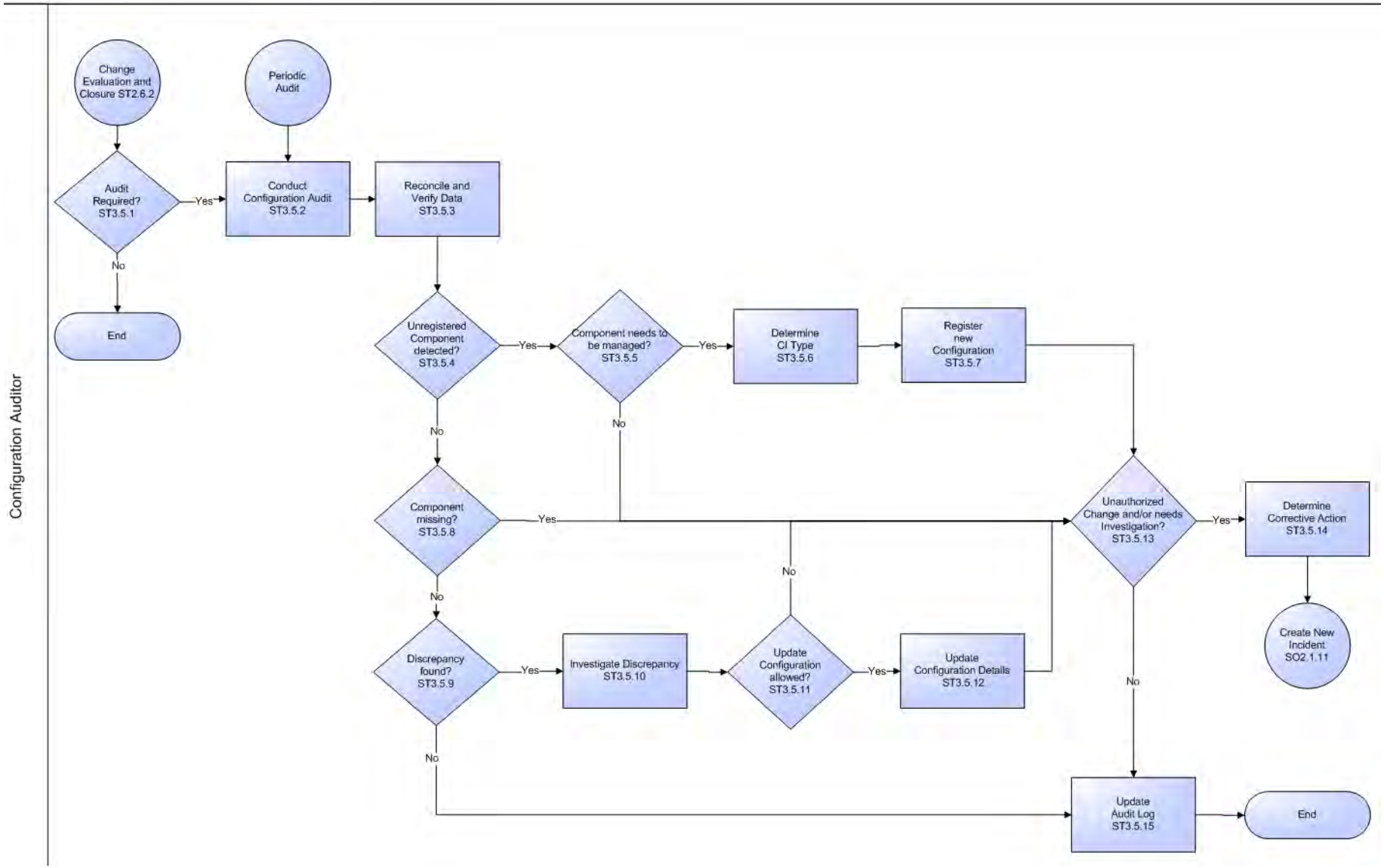

Figure 15-5 Configuration Verification and Audit workflow

Table 15-5 Configuration Verification and Audit process

Process ID	Procedure or Decision	Description	Role
ST 3.5.1	Audit required?	Configuration audits should be considered before and after a major change or release.	Configuration Auditor
ST 3.5.2	Conduct configuration audit	Configuration audits (manual or automated) are scheduled periodically. The audit verifies each individual CI. It uses an automated inventory tool that scans the system. Another method is to scan the IT environment and discover the component connected to the enterprise. New components may be discovered, requiring management in the CMS.	Configuration Auditor
ST 3.5.3	Reconcile and verify data	Collected data from the audit must be reconciled and compared with the data already stored in the CMS. Different reconciliation keys and rules can be applied to match the discovered item with the CI in the CMS.	Configuration Auditor
ST 3.5.4	Unregistered component detected?	An unregistered component may be detected in cases where the item cannot be matched and found in the CMS. If an unregistered component is detected, go to ST 3.5.5. If not, continue with ST 3.5.8.	Configuration Auditor
ST 3.5.5	Component needs to be managed?	Determine whether the new component needs to be registered in the CMS, based on the scope of the CMS. If yes, continue with ST 3.5.6. If no, go to ST 3.5.13.	Configuration Auditor
ST 3.5.6	Determine CI type	The CI type is selected, based on the properties of the discovered component (for example, model name or type of device).	Configuration Auditor
ST 3.5.7	Register new configuration	Create a new CI. Enter the additional attributes of the CI, based on the audit data. Go to ST 3.5.13.	Configuration Auditor
ST 3.5.8	Component missing?	If a component cannot be discovered during an audit, it may be lost or stolen (for example, the CI has not been connected to the network for some period of time). The audit status is updated to Lost. If yes, continue with ST 3.5.13. If no, continue with ST 3.5.9.	Configuration Auditor
ST 3.5.9	Discrepancy found?	Based upon the comparison between the CMS administration and the actual data from the audit, one or more discrepancies may be detected. If yes, continue with ST 3.5.10. If not, continue with ST 3.5.15.	Configuration Auditor
ST 3.5.10	Investigate discrepancy	The mismatch between the CMS administration and the actual configuration is investigated in more detail. For each discrepancy, attribute differences and relationships are investigated.	Configuration Auditor
ST 3.5.11	Update configuration allowed?	To reduce the number of manual activities, some fields are populated by discovery and auditing tools. These attributes will not be maintained manually. Determine whether the differences can be updated directly without a formal change procedure. If yes, continue with ST 3.6.12. If no, go to ST 3.5.13.	Configuration Auditor
ST 3.5.12	Update configuration details	The configuration details are updated, based on the audit date to ensure that the administration is correctly reflecting the actual situation.	Configuration Auditor

Table 15-5 Configuration Verification and Audit process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 3.5.13	Unauthorized change or needs investigation?	Determine whether the mismatch between the audit and the CMS administration requires further investigation (for example, detection of unauthorized software). If yes, go to ST 3.5.14. If no, continue with ST 3.5.15.	Configuration Auditor
ST 3.5.14	Determine corrective action	Document the discrepancy and determine the appropriate actions (for example, additional investigation is needed). An incident must be created and assigned to the person responsible for executing the actions. Follow SO 2.1.11 to create a new incident.	Configuration Auditor
ST 3.5.15	Update audit log	The CI is updated with the audit status and last audit date.	Configuration Auditor

Master data management (process ST 3.6)

Master reference data is key data that the Configuration Management System (CMS) depends on and is often provided by different organizational functions, such as human resources management, finance, and facilities. For example, master data can include details about organization units, cost centers, employee data, and locations.

The objective of the Master data management process is to reconcile master reference data managed in other administrations. Modification of this reference data is processed in the (CMS).

Changes in organizational structures, locations, and employee data might result in exceptions or incidents, because existing Configuration Items (CIs) and contracts remain associated with these entities (for example, the retirement of an employee who still has a laptop or mobile phone assigned). Modification of this data must be reviewed and appropriate actions should be initiated.

Details for this process can be seen in the following figure and table.

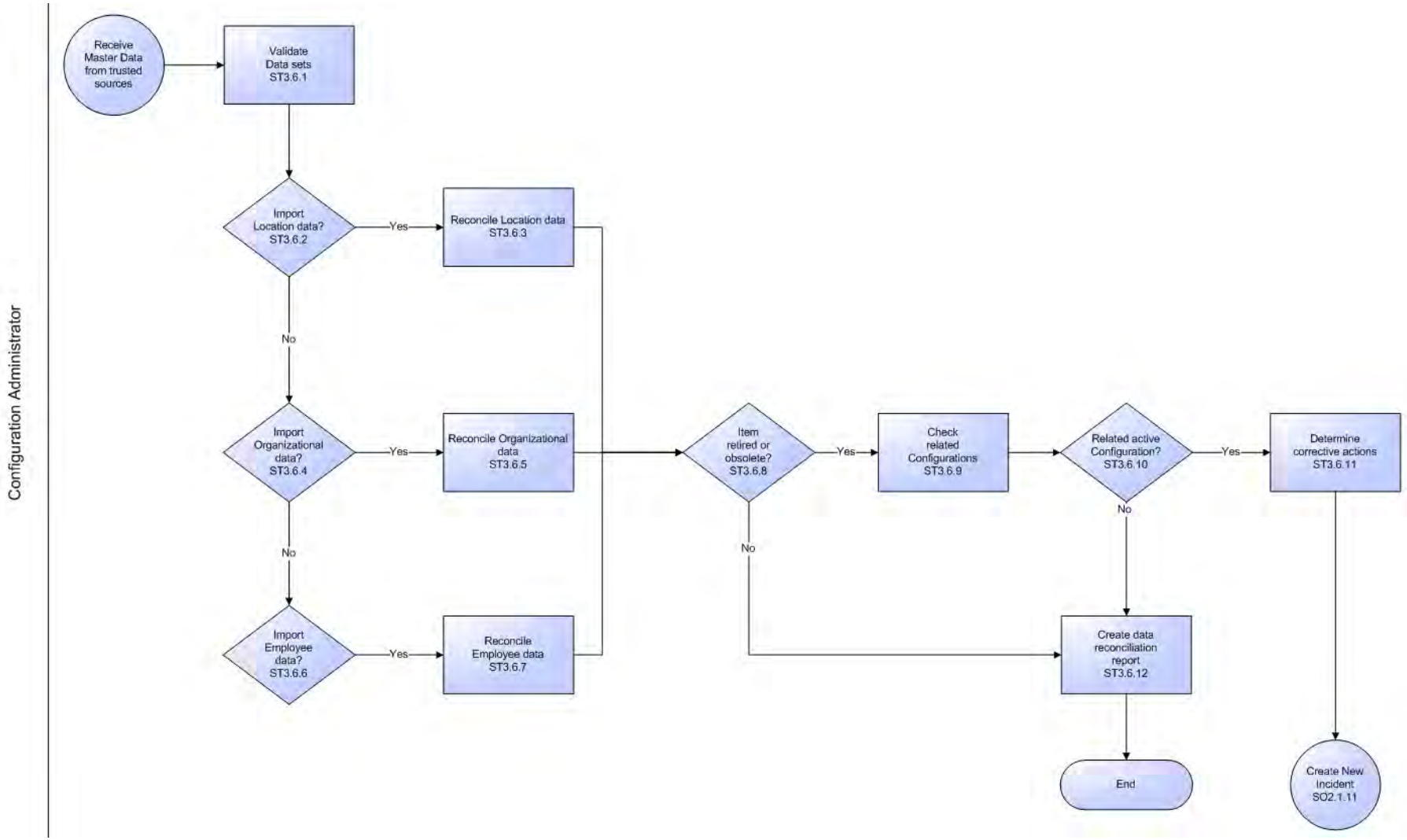

Figure 15-6 Master data management workflows

Table 15-6 Master data management process

Process ID	Procedure or Decision	Description	Role
ST 3.6.1	Validate data sets	Periodically data sets are received from trusted sources. The Configuration Administrator checks the format and content against the defined specifications.	System Administrator Configuration Administrator
ST 3.6.2	Import location data?	If you want to import location data, continue with ST 3.6.3. If not, go to ST 3.6.4.	System Administrator Configuration Administrator
ST 3.6.3	Reconcile location data	Import and load location data into the CMS.	System Administrator Configuration Administrator
ST 3.6.4	Import organizational data?	If you want to import organizational data, continue with ST 3.6.5. If not, go to ST 3.6.6.	System Administrator Configuration Administrator
ST 3.6.5	Reconcile organizational data	Import and load organizational data into the CMS.	System Administrator Configuration Administrator
ST 3.6.6	Import employee data?	If you want to import employee data, continue with ST 3.6.7. If not, stop.	System Administrator Configuration Administrator
ST 3.6.7	Reconcile employee data	Import and load employee data into the CMS.	System Administrator Configuration Administrator
ST 3.6.8	Item retired or obsolete?	Verify that one or more items in the data set are retired or no longer present. Make sure to update the status of items in the CMS.	System Administrator Configuration Administrator

Table 15-6 Master data management process (cont'd)

Process ID	Procedure or Decision	Description	Role
ST 3.6.9	Check related configurations	Verify that one or more CIs are still related to retired items in the modified master data record. For example, a retired user may still have one or more subscriptions or CIs for which that user is responsible. Updates of interest include: • Status updates (for example, retirement) • Job profile changes (for validating access rights and related current subscriptions) • Reorganizations (for example, merge or split of departments) • Cost center changes Master data modifications must be verified to ensure that these updates do not conflict with configuration administration.	System Administrator Configuration Administrator
ST 3.6.10	Related active configuration?	If there is a related active configuration, continue with ST 3.6.11. If not, go to ST 3.6.12.	System Administrator Configuration Administrator
ST 3.6.11	Determine corrective actions	Follow the procedure to create a new incident (see SO 2.1.11).	System Administrator Configuration Administrator
ST 3.6.12	Create data reconciliation report	Create a report with a summary of data modifications and reconciliation errors, which includes statistics of the number of modifications (for example, new items and retired items).	System Administrator Configuration Administrator

16 Configuration Management Details

HP Service Manager uses the Configuration Management application to enable the Configuration Management process. The main function of Configuration Management is to identify, baseline, and maintain the Configuration Items (CIs) and to control changes to them. It also ensures that formal approvals guide releases into controlled environments and operational uses.

This section explains to the administrator or developer how selected Configuration Management fields are implemented in the out-of-box Service Manager system.

Topics in this section include:

MyDevices configuration item form

The Configuration Manager can view and edit details about a CI on the Configuration item form.

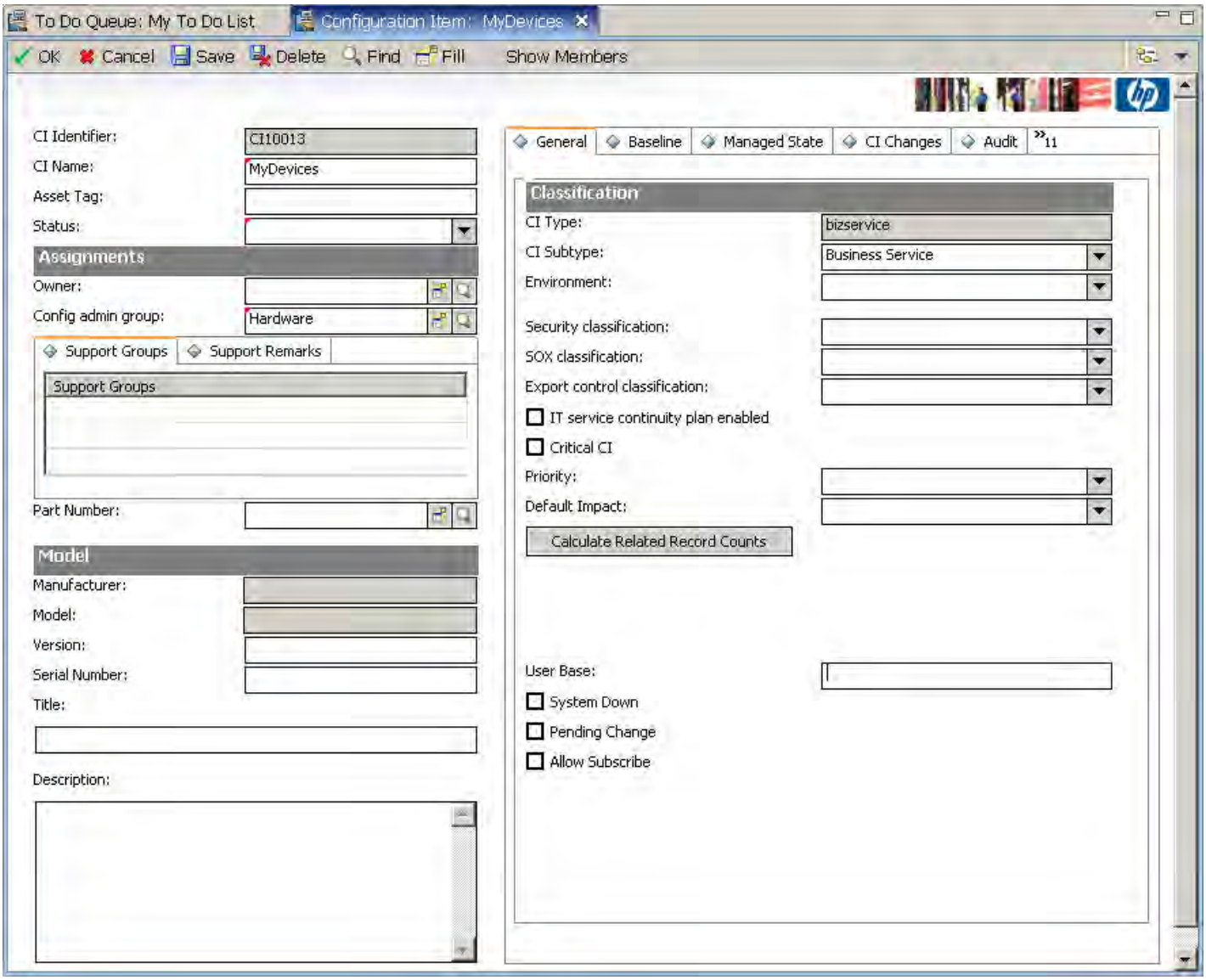

Figure 16-1 MyDevices configuration item form

Configuration Management form details

The following table identifies and describes the fields on the Configuration Management forms.

Table 16-1 Configuration Management field descriptions

Label	Description
CI Identifier	System-generated field that specifies the unique ID of the configuration item (CI).
CI Name	The name of the CI. This is a required field.
Asset Tag	This is a legacy field intended for customers migrating from previous versions of Service Manager to track the label or tag placed on physical assets, such as for example, a bar code.
Status	This field specifies the status of the CI. The out-of-box data is: • Available • Planned/On order • Received • In Stock • Reserved • In use • Maintenance • Disposed/Retired • Installed The field is updated manually to reflect the current status of the CI. This is a required field. The Installed status is the default status.
Assignments > Owner	This field identifies the department that owns the CI, for example, the HR department could own the laptops that its employees use.
Assignments > Config admin group	This field identifies the group responsible for supporting the CI while the Owner identifies the department that owns the CI. For example, a PC is owned by the HR department, but IT is the Config admin group responsible for supporting the CI. It is the assignment group responsible for handling interactions or incidents for the CI. This is a required field.
Assignments > Support Groups	This field identifies what assignment groups receive tickets when this CI is part of an interaction as well as when escalating to an incident.
Assignments > Support Remarks	This field is a comment field intended to describe or provide notes for the support groups.
Assignments > Part Number	This field specifies the inventory component number for the CI as defined by the company-defined CI inventory number in the model table. The system uses this number to provide data on the Manufacturer, Model, and Version fields if available.
Model > Manufacturer	This is a system-generated field that specifies the manufacturer of the CI if one is associated with the Part Number. This field along with model and serial number uniquely identify the CI.
Model > Model	This is a system-generated field that specifies the manufacturer's model if one is associated with the Part Number. This field along with manufacturer and serial number uniquely identify the item.

Table 16-1 Configuration Management field descriptions (cont'd)

Label	Description
Model > Version	This field specifies the manufacturer's version number for the CI.
Model > Serial Number	This field specifies the manufacturer's serial number for the CI.
Model > Title	This field specifies the title of the primary user of the CI; for example Mr. or Mrs.
Model > Description	This field is a free-form text field to add additional information about the CI.
Classification > CI Type	This field identifies the type of CI. The out-of-box data is: • Application • Business Service • CI Group • Computer • Display Device • Example • Furnishings • Hand Held Devices • Mainframe • Network Components • Office Electronics • Software License • Storage • Telecommunications The Managed State notebook tab displays different fields depending up the CI type selected.
Classification > CI Subtype	This field identifies the subtype of CI. The list of available subtypes depends upon the CI Type the user selected. For more information see Table 16-2 on page 228.
Classification > Environment	This field specifies if a CI belongs to a particular environment. The out-of-box data is: • Development • Test • Production • Failover • None
Classification > Security classification	This field specifies if the CI has any security restrictions. The out-of-box data is: • Unrestricted • Restricted • Confidential • Most Confidential

Table 16-1 Configuration Management field descriptions (cont'd)

Label	Description
Classification > OX classification	This field specifies if the CI has a Sarbanes Oxley (SOX) classification that applies to the CI. The out-of-box data is: • Critical • Non Critical
Classification > Export control classification	This field specifies if the CI has an Export Control classification. The out-of-box data is: • EAR99 (Non Controlled) • 4D994 • 5D991 • 5D002 • 5D992
Classification > IT service continuity plan enabled	This field specifies if the CI has an IT service continuity plan enabled for it.
Classification > Critical CI	This field specifies if the CI is critical for day-to-day operation, such as an E-mail server or RDBMS server. If you open an incident on a critical CI, the incident ticket indicates that this is a critical CI.
Classification > Priority	This field specifies the default priority of any related records opened against the CI. The information in this field is used to prepopulate the priority in an incident or interaction. When a user selects the CI in an incident or interaction, it populates the incident or interaction priority based on the CI priority field. The out-of-box data is: • 1 - Critical • 2 - High • 3 - Average • 4 - Low For additional information see, Table 7-1 on page 86.
Classification > Default Impact	This field specifies the default impact of any related record opened against the CI. the information in this field is used to prepopulate the impact in an incident or interaction. When a user selects the CI in an incident or the interaction, it populates the incident or interaction impact based on the CI Default Impact field. The out-of-box data is: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User For additional information see, Table 7-1 on page 86.
Classification > Calculate Related Record Counts	This field displays a count of related incidents, problems, known errors, and changes that were opened against this CI.
Classification > User Base	This field displays a count of the number of users who use the CI.
Classification > System Down	This field indicates whether the CI is currently operational or has an open incident related to it causing it to be non-operational. When you close the incident ticket for the CI, this action clears the flag. The CI is no longer marked as down.

Table 16-1 Configuration Management field descriptions (cont'd)

Label	Description
Classification > Pending Change	This field indicates whether or not there are any changes pending against this CI. When you close or open a change for the CI, this action sets or clears the flag.
Classification > Allow Subscribe	This field determines if the CI is available for subscriptions from the Service Catalog.
Baseline > Baseline	This field indicates if the CI has an associated baseline and if the CI is in compliance.
Baseline > Baseline Version	This field indicates the baseline version that the CI is tracked against. Baseline Versions enable you to have CIs with the same baseline configuration but slight differences. You can have several versions of that baseline, or if you have updates for a new version of a software installed, then you can select a specific version of a baseline for a CI.
Managed State	This notebook tab lists the expected values of CI attributes. All changes to fields in the Managed State notebook tab require a Change Management record. See Table 16-3 on page 231 for the Managed State sub-tab field descriptions.
Actual State	This notebook tab lists the actual values of CI attributes if the Service Manager system has an integration to HP Universal CMDB It shows the latest discovered information from the UCMDB or its sources.
CI Changes > Pending Attribute Changes	This field lists the attributes that are waiting to be changed through a Change Management record or changes requested through an Unplanned Change (requires an HP Universal CMDB integration). The data in this field can only be modified through Change Management. Each CI has a set of managed attributes that can be changed through Change Management.
CI Changes > Historic Attribute Changes	This field lists the attributes that are have already been changed through a Change Management record or changes requested through an Unplanned Change (requires an HP Universal CMDB integration).
Relationships > Upstream Configuration Item, Relationship Name, Relationship Type, Relationship Subtype	This field shows information about which upstream CIs are dependent on the selected CI. Upstream CIs depend on the current CI. For example, the upstream E-mail service depends on the downstream E-mail server, the network, and your E-mail program.
Relationships > Add upstream relationship	This option links to the add a new CI relationship record that enables you to add a new upstream relationship to this CI.
Relationships > Show Logical	This option displays all logical CI relationships for the specified CI. A logical connection mean that you can access the CI but there is no direct physical connections to other CIs. For example, a network printer that you use.
Relationships > Show Physical	This option displays all physical CI relationships for the specified CI. A physical connection is when a CI is directly attached to another device. For example, a PC connected to a dedicated printer with printer cable.
Relationships > Show All	This option displays all CI relationships for this CI that are of either physical or logical.
Relationships > Downstream Relationships > Relationship Name, Relationship Type, Relationship Subtype	This option shows the CIs that have a downstream dependency on this CI. For example, the upstream E-mail service depends on the downstream E-mail server, the network, and your E-mail program.

Table 16-1 Configuration Management field descriptions (cont'd)

Label	Description
Relationship Graph	This notebook tab displays a graphical representation of the upstream and downstream relationships for the CI.
Subscribers > Subscriber, Type, Status	This is a system-generated notebook tab that shows all the subscriptions (people or departments) made against the CI, and the status of the subscription. Example: People and departments can subscribe to Services or CIs. When looking at an interaction, the Service Desk Agent views a list of all the CI the caller is subscribed to, and their current status.
Audit > Audit Policy, Audit Status, Audit Discrepancy, Last Audit Date, Next Scheduled Audit, Last Audited By	These fields display auditing information and are only enabled for those users who have the capability to audit CIs. The user role is Configuration Auditor.
Software > Applications & Drivers	This notebook tab displays information about the software and drivers installed on the CI. For example, a PC might list Microsoft Office and Adobe Reader along with the version, install date, and license ID for each. An Administrator enters this data using he Managed Software menu.
Primary User > Primary Contact & Support Contacts	This field displays the primary user who is the person assigned the CI and uses it on a day-to-day basis. Support contacts are secondary contacts who may have access to the CI. For example, a subscriber would be a department for a printer, but the users would be all the people who use the printer to print. The primary user is the person who is responsible for the printer, such as the department manager.
Location > Location Information & Location Comments	This notebook tab describes the physical location of the CI and may include information such as special access requirements (for example, you may require badge access or you may need to be accompanied by authorized personnel in some locations). For example, the location information might contain, Australia, Home Site, main building, second floor, room 3.
Vendor > Vendor Information, Address, & Contract and Response Information	This notebook tab provides vendor information about the CI for support and maintenance. When the user enters the vendor name, the system provides the additional details.
Metrics > Outage History, Uptime Objectives, Max Duration Objectives	This notebook tab displays information related to the SLA and SLO availability data for the CI.
Financial > Contracts, Expense Lines, Labor, Parts	This notebook tab displays information for the service contracts, parts, labor, and expenses for the CI.
Scanner	This notebook tab provides information about any scanning done on the CI. The information includes the last time this CI was scanned and the date and time of the scan. Scanning can be done to detect viruses or determine the software installed on the CI.

Configuration Item types and subtypes

The following table lists the types and subtypes available for the out-of box Configuration Item (CI) Names.

Table 16-2 Configuration Item types and subtypes

CI Name	CI Type	CI Subtype
Application	application	Anti-Virus / Security Back-up Business Development Tools Entertainment Graphics Internet/Web Networking Operating System Reference Other
Business Service	bizservice	Business Service Application Service Infrastructure Service
CI Group	cigroup	Ad Hoc Baseline
Computer	computer	Desktop Dumb Terminal Laptop Tower MAC Server Host VAX Windows Unix Mainframe Logical Partition Terminal Server
Display Device	displaydevice	Monitor Projector
Example	example	
Furnishings	furnishings	Artwork Armoire Bookcase Chair Computer Desk Desk Collection File Cabinet Meeting Table
Hand Held Devices	handhelds	PDA Cell Phone Pager Blackberry Device GPS Device

Table 16-2 Configuration Item types and subtypes (cont'd)

CI Name	CI Type	CI Subtype
Mainframe	mainframe	Controller Host CPU FEP NCP LPAR
Network Components	networkcomponents	Router Hub Switch Modem Network Interface Card Gateway Firewall Network Component ATM Switch RAS LB Concentrator Net Device Switch Router
Office Electronics	officeelectronics	Copy Machine Printer Fax Machine Paper Shredder Camera Speaker Calculator Multifunction Word Processor Typewriter VCR Television UPS Net Printer

Table 16-2 Configuration Item types and subtypes (cont'd)

CI Name	CI Type	CI Subtype
Software License	softwarelicense	DBMS License Development Tool License Enterprise Management License Operating System License Outlook Productivity Tools License Project Management License Utility Software License
Storage	storage	CDRW Direct Attached Storage (DAS) HDD Network Attached Storage (NAS) Storage Area Network (SAN) ZIP CD Burner
Telecommunications	telcom	Desk Phone Flush Wall Mount Headsets & Accessories NBX PBX Paging Solution Surface Mount

Managed State Subtabs

The Managed State tab uses sub-tabs to display data about each CI. There are three sub-tabs for this purpose, The Network sub-tab and the Additional sub-tab are used for all CI types. The third sub-tab depends upon the CI and CI type selected. For example, the Adobe Reader is an application CI type and therefore includes the Application sub-tab on the Managed State tab.

The following table outlines the sub-tabs and fields available for the different CI types.

Table 16-3 Managed State sub-tabs

Sub-Tab	Visible Condition	Field Label	Field Name
Hardware	Type: computer or Type: networkcomponents or Type: officeelectronics	Machine Name Primary MAC Address Additional MAC Addresses OS Name OS Manufacturer OS Version Bios ID Bios Manufacturer Bios Model Physical Memory (Kb)	machine.name mac.address addlMacAddress operating.system os.manufacturer os.version bios.id bios.manufacturer bios.model physical.mem.total
Network	true	Network Name Primary IP Address Subnet Mask Default Gateway Configuration File Addl IP Address Addl Subnet Mask	network.name ip.address subnet.mask default.gateway config.file addlIPAddress addlSubnet
Application	Type: application	Application Name Administration URL/Port Business Import Level Disaster/Recovery Coverage Disaster/Recovery Tier Primary Directory Path Data Classification Product Version License Type Service Hours Notification Group	ci.name admin.urlport bu siness.import.level disaster.coverage recorvery.tier primary.path data.classification product.version license.type service.hours notification.groups
Database	Type: database	Data Privacy Data Classification Port Number Disaster/Recovery Coverage Disaster/Recovery Tier Administration URL/Port Product Version Listener Access Port Notification Group	data.privacy recorvery.tier port.number NULL recorvery.tier admin.urlport product.version listener.port notification.group

Table 16-3 Managed State sub-tabs (cont'd)

Sub-Tab	Visible Condition	Field Label	Field Name
Telecom	Type: telecom	Admin ID Admin Password Remote Access Phone Remote Access IP Voice type Disaster/Recovery Coverage Disaster/Recovery Tier Grid Login Server Name Monitored	admin.id admin.password remote.phone remote.ip NULL disaster.recovery recorvery.tier grid login.server.name monitored
Service	Type: bizservice	Service Name Service Type Service Status Allow Subscriptions Administration URL/Port Business Import Level Disaster/Recovery Coverage Disaster/Recovery Tier Primary Directory Path	ci.name subtype service.status allowSubscription admin.urlport NULL NULL recorvery.tier primary.path
Additional	true	Manufacturer Name Type Description	addl.manufacturer addl.name addl.type addl.description

A Compliance with Industry Standards

Service Manager's compliance with ISO 20000

ISO 20000-2 (that is, Part 2) is a "Code of Practice" that describes the recommendations for service management within the scope of ISO 20000-1. The following table shows the Service Manager best practice coverage of the items in the Code of Practice.

Table A-1 Service Manager coverage of the ISO 20000 Code of Practice

ISO 20000 Code of Practice	Service Manager Best Practices Coverage
Resolution processes	
7.2 Business Relationship Management	
7.2.1 Service Complaints	Incident Management > Complaint Handling (SO 2.9)
8.1 Background	
8.1.1 Setting Priorities	Interaction Management > Interaction Handling (SO 0.2) Priority is based on impact and urgency. Target date is set according to SLAs
8.1.2 Workarounds	• Problem Management > Problem Detection, Logging, and Categorization (SO 4.1) • Problem Management > Problem Investigation and Diagnosis (SO 4.3) • Problem Management > Known Error Logging and Categorization (SO 4.4) • Problem Management > Known Error Investigation (SO 4.5) Logging and maintenance of workarounds is performed in all of the procedures above
8.2 Incident Management	
8.2.1 General	
Proactive and reactive process, responding to incidents that affect, or potentially could affect the service	Incident Management > Incident Logging (SO 2.1) Incidents can be created based on user interactions as well as based on events.
Concerned with the restoration of the customers' service, not with determining the cause of incidents.	Incident Management > Incident Resolution and Recovery (SO 2.4) Incidents are preferably solved by means of a workaround leaving the structural solution to the Problem Management process.
The Incident Management process should include the following:	

Table A-1 Service Manager coverage of the ISO 20000 Code of Practice (cont'd)

ISO 20000 Code of Practice	Service Manager Best Practices Coverage
a) call reception, recording, priority assignment, classification	Interaction Management > Interaction Handling (SO 0.2)
b) first line resolution or referral	Interaction Management > Interaction Handling (SO 0.2)
c) consideration of security issues	Interaction Management > Interaction Handling (SO 0.2) Security is one of the areas that you can select when registering an interaction.
d) Incident tracking and lifecycle management	• Incident Management > Monitor SLA (SO 2.7) • Incident Management > OLA and UC Monitoring (SO 2.8)
e) Incident verification and closure	Interaction Management > Interaction Closure (SO 0.3)
f) first line customer liaison	Interaction Management > Interaction Handling (SO 0.2)
g) escalation	Incident Management > Incident Escalation (SO 2.6)
Incidents may be reported by telephone calls, voice mails, visits, letters, faxes or email, or may be recorded directly by Users with access to the incident ticketing system, or by automatic monitoring software.	• Interaction Management > Self-Service by User (SO 0.1) • Interaction Management > Interaction Handling (SO 0.2)
Progress (or lack of it) in resolving incidents should be communicated to those actually or potentially affected.	Incident Management > Incident Escalation (SO 2.6)
Final closure of an incident should only take place when the initiating User has been given the opportunity to confirm that the incident is now resolved and service restored.	Interaction Management > Interaction Closure (SO 0.3)
8.2.2 Major Incidents	
There should be a clear definition of what constitutes a major incident and who is empowered to invoke Changes to the normal operation of the incident/Problem process.	• Incident Management > Monitor SLA (SO 2.7) • Incident Management > OLA and UC Monitoring (SO 2.8) Escalation triggers are clearly defined, including the process roles responsible for triggering the escalation.
All major incidents should have a clearly defined responsible manager at all times	Incident Management > Incident Escalation (SO 2.6) The responsible process roles for this procedure are clearly defined.
8.3 Problem management	
8.3.1 Scope of Problem Management	Problem Management (SO 4)
8.3.2 Initiation of Problem Management	
Incidents should be classified to help determine the causes of Problems. Classification may reference existing Problems and Changes.	Incident Management > Incident Closure (SO 2.5). Upon closure the incident classification should be reviewed and adjusted if needed.

Table A-1 Service Manager coverage of the ISO 20000 Code of Practice (cont'd)

ISO 20000 Code of Practice	Service Manager Best Practices Coverage
8.3.3 Known Errors	• Problem Management > Known Error Logging and Categorization (SO 4.4) • Problem Management > Known Error Investigation (SO 4.5) • Problem Management > Known Error Solution Acceptance (SO 4.6) • Problem Management > Known Error Resolution (SO 4.7)
8.3.4 Problem Resolution	Problem Management > Known Error Solution Acceptance (SO 4.6). The implementation of the solution is requested to the Change Management process
8.3.5 Communication	• Interaction Management > Interaction Handling (SO 0.2) Matching with published Known errors takes place. • Incident Management > Incident Investigation and Diagnosis (SO 2.3) Matching with published known errors takes place. • Problem Management (SO 4) Known error information is logged and maintained throughout the whole Problem Management process.
8.3.6 Tracking and Escalation	Problem Management > Problem and Known Error Monitoring (SO 4.9)
8.3.7 Incident and Problem Ticket Closure	Problem Management > Problem Closure and Review (SO 4.8)
8.3.8 Problem Reviews	Problem Management > Problem Closure and Review (SO 4.8)
8.3.9 Topics for Reviews	Problem Management > Problem Closure and Review (SO 4.8)
8.3.10 Problem Prevention	Problem Management > Problem Detection, Logging, and Categorization (SO 4.1)
Control Processes	
9.1 Configuration Management	
9.1.1 Configuration Management Planning and implementation	Configuration Management > Configuration Management Planning (ST 3.1)
9.1.2 Configuration Identification	Configuration Management > Configuration Identification (ST 3.2)
9.1.3 Configuration Control	Configuration Management > Configuration Control (ST 3.3)
9.1.4 Configuration Status Accounting and Reporting	Configuration Management > Configuration Status Accounting and Reporting (ST 3.4)
9.1.5 Configuration Verification and Audit	Configuration Management > Configuration Verification and Audit (ST 3.5)
9.2 Change Management	
9.2.1 Planning and Implementation	• Change Management > Change Assessment and Planning (ST 2.3) • Change Management > Change Approval (ST 2.4) • Change Management > Coordinate Change Implementation (ST 2.5)

Table A-1 Service Manager coverage of the ISO 20000 Code of Practice (cont'd)

ISO 20000 Code of Practice	Service Manager Best Practices Coverage
9.2.2 Closing and Reviewing the Change request	Change Management > Change Evaluation and Closure (ST 2.6)
9.2.3 Emergency Changes	Change Management > Emergency Change Handling (ST 2.7)
9.2.4 Change Management Reporting, Analysis and Actions	Change Management > Change Evaluation and Closure (ST 2.6)

Service Manager's compliance with COBIT 4.1

The following table shows the mapping between the applicable COBIT 4.1 controls and the coverage of these controls in the Service Manager best practices. The control objectives are identified by a two-character domain reference (PO, AI, DS and ME). plus a process number and a control objective number. For more information about the COBIT 4.1 controls, see the official COBIT 4.1 documentation.

Table A-2 Service Manager's coverage of COBIT 4.1 Controls

COBIT Control	Service Manager best practices coverage
PO4 Plan and Organize	
PO4.1 IT Process Framework	Level 0 > Processes
PO4.6 Establishment of Roles and Responsibilities	Level 0 > Organizational Model
PO4.11 Segregation of Duties	• Level 0 > Organizational Model > Process Roles • Change Management > Emergency Change Handling (ST 2.7) Releasing a new application in case of an Emergency Change Handling situation is performed by the Release Packaging and Build Manager (another Change Analyst). • Configuration Management > Configuration Management Planning (ST 3.1) Maintenance of CI types is performed by another role than the role adding or modifying the Configuration
AI6 Manage Changes	
AI6.1 Change Standards and Procedures	Change Management (ST 2)
AI6.2 Impact Assessment, Prioritization and Authorized	• Change Management > Change Approval (ST 2.4) • Change Management > Change Assessment and Planning (ST 2.3)
AI6.3 Emergency Changes	Change Management > Emergency Change Handling (ST 2.7)
AI6.4 Change Status Tracking and Reporting	• Change Management > Change Logging (ST 2.1) Enables the logging of Changes in the Service management tool Change Management. • Change Management > Change Assessment and Planning (ST 2.3) Planning is created which' after approval' leads the Change implementation.
AI6.5 Change Closure and Documentation	Change Management > Change Evaluation and Closure (ST 2.6)
DS1 Define and Manage Service Levels	
DS1.2 Definition of Services	Configuration Management (ST 3) Business Services are stored in the Configuration Management System and related to the CI's supporting the Service.
DS1.3 Service Level Agreements	Incident Management > Monitor SLA (SO 2.7) The main aspect of the Service Manager best practices and the Configuration of Service Manager is its Service orientedness. Target response times for all Interactions and related tickets are set according to SLAs with the user's representatives.

Table A-2 Service Manager's coverage of COBIT 4.1 Controls (cont'd)

COBIT Control	Service Manager best practices coverage
DS1.4 Operating Level Agreements	Incident Management > OLA and UC Monitoring (SO 2.8) Service Manager is configured to enable measurement of OLSs
DS2 Manage Third-party Services	
DS2.4 Supplier Performance Monitoring	Incident Management > OLA and UC Monitoring (SO 2.8) Service Manager is configured to enable measurement of UCs.
DS8 Manage Service Desk and Incidents	
DS8.1 Service Desk	Interaction Management > Interaction Handling (SO 0.2)
DS8.2 Registration of Customer Queries	Interaction Management > Interaction Handling (SO 0.2)
DS8.3 Incident Escalation	Incident Management > Incident Escalation (SO 2.6)
DS8.4 Incident Closure	• Incident Management > Incident Closure (SO 2.5) • Interaction Management > Interaction Closure (SO 0.3)
DS9 Manage the Configuration	
DS9.1 Configuration Repository and Baseline	Configuration Management (ST 3)
DS9.2 Identification and Maintenance of Configuration Items	• Configuration Management > Configuration Identification (ST 3.2) • Configuration Management > Configuration Control (ST 3.3) • Configuration Management > Master data management (ST 3.6)
DS9.3 Configuration Integrity Review	• Configuration Management > Configuration Status Accounting and Reporting (ST 3.4) • Configuration Management > Configuration Verification and Audit (ST 3.5)
DS10 Manage Problems	
DS10.1 Identification and Classification of Problems	• Problem Management > Problem Detection, Logging, and Categorization (SO 4.1) • Problem Management > Problem Prioritization and Planning (SO 4.2) • Problem Management > Known Error Logging and Categorization (SO 4.4)
DS10.2 Problem Tracking and Resolution	• Problem Management > Problem Investigation and Diagnosis (SO 4.3) • Problem Management > Known Error Investigation (SO 4.5) • Problem Management > Known Error Solution Acceptance (SO 4.6) • Problem Management > Problem and Known Error Monitoring (SO 4.9).
DS10.3 Problem Closure	• Problem Management > Known Error Resolution (SO 4.7) • Problem Management > Problem Closure and Review (SO 4.8)
DS10.4 Integration of Configuration, Incident and Problem Management	Problem Management > Problem Detection, Logging, and Categorization (SO 4.1) Problems are identified based on incident tickets.

B Service Manager tables

Service Desk application tables and fields

Most fields important for the Service Desk application are located in the incidents table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the incidents table.

Table B-1 Important fields in the incidents table

Label	Field Name
Interaction ID	incident.id
Primary Contact > Contact for this interaction	callback.contact
Primary Contact > Notify By	callback.type
Service Recipient > This interaction is for	contact.name
Affected Items > Service	affected.item
Affected Items > Affected CI	logical.name
Title	title
Description	description
Interaction Detail tab	category
Interaction Detail tab > Category	category
Interaction Detail tab > Area	subcategory
Interaction Detail tab > Sub-area	product.type
Interaction Detail tab > Impact	initial.impact
Interaction Detail tab > Urgency	severity
Interaction Detail tab > Priority	priority.code

Table B-1 Important fields in the incidents table (cont'd)

Label	Field Name
Interaction Detail tab > Knowledge Source	kpf.id
Interaction Detail tab > Closure Code	resolution.code
Interaction Detail tab > Solution	resolution
Status	open
Approval Status	approval.status

Incident Management application tables and fields

Most fields important for the Incident Management application are located in the probsummary table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the probsummary table.

Table B-2 Important fields in the probsummary table

Label	Field Name
Incident ID	number
Status	problem.status
Assignment > Assignment Group	assignment
Assignment > Assignee	assignee.name
Assignment > Vendor	vendor
Assignment > Reference Number	reference.no
Affected Items > Services	affected.item
Affected Items > Affected CI	logical.name
Affected Items > Critical CI	device.severity
Affected Items > Pending Change	pending.change
Affected Items > CI is operational (no outage)	operational.device

Table B-2 Important fields in the probsummary table (cont'd)

Label	Field Name
Affected Items > Outage Start	downtime.start
Affected Items > Outage End	downtime.end
Location	location.full.name
Title	brief.description
Description	action
Incident Detail > Category	category
Incident Detail > Area	subcategory
Incident Detail > Sub-area	product.type
Incident Detail > Impact	initial.impact
Incident Detail > Urgency	severity
Incident Detail > Priority	priority.code
Incident Detail > Service Contract	contract.id
Incident Detail > SLA target Date	next.breach
Incident Detail > Alert Status	status
Incident Detail > Problem Management Candidate	prob.mgmt.candidat
Incident Detail > Candidate for Knowledge DB	solution.candidate
Incident Detail > Closure Code	resolution.code
Incident Detail > Solution	resolution
Affected Services tab	affected.services

Problem Management application tables and fields

The Problem Management application divides the problem management process into two stages. Problem Control, which identifies and tracks problems, and Error Control, which controls the process of finding solutions.

The Problem Management application stores the data for problem and Error Control in separate tables, as documented below.

- Problem Control on page 242
- Error Control on page 244

Problem Control

Many important fields for the Problem Management application are located in the rootcause table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the rootcause table.

Table B-3 Important fields in the rootcause table

Label	Field Name
Problem ID	id
Phase	current.phase
Status	rcStatus
Assignment > Assignment Group	assignment
Assignment > Problem Coordinator	asignee.name
Affected Items > Services	affected.item
Affected Items > Primary CI	logical.name
Affected Items > Affected CI Count	affected.ci.count
Title	brief.description
Description	description
Root Cause Description	root.cause
Problem Detail > Category	incident.category Note: The problem category is not displayed on the problem forms. The category displayed on the problem forms is the Incident category.
Problem Detail > Area	subcategory

Table B-3 Important fields in the rootcause table (cont'd)

Label	Field Name
Problem Detail > Sub-area	product.type
Problem Detail > Impact	initial.impact
Problem Detail > Urgency	severity
Problem Detail > Priority	priority.code
Problem Detail > SLA Target Date	next.breach
Problem Detail > Root Cause Target Date	rootcauseDate
Problem Detail > Solution Target Date (Solution Identification Date)	solutionDate
Problem Detail > Resolution Target Date (Problem Resolution Date)	expected.resolution.time
Problem Detail > Related Incident Count	incident.count
Incident Detail > Closure Code	closure.code
Problem Detail > Suggested Workaround	workaround
Assessment > Estimated # of Mandays	estimatedMandays
Assessment > Estimated Costs	estimatedCost
Assessment > Affected CI's table	affected.ci

Error Control

Another important table in the Problem Management application is the knownerror table. The known error forms use the fields from the knownerror table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the knownerror table.

Table B-4 Important fields in the knownerror table

Label	Field Name
Known Error ID	id
Phase	current.phase
Status	rcStatus
Assignment > Assignment Group	assignment
Assignment > Problem Coordinator	assignee.name
Affected Items > Services	affected.item
Affected Items > Primary CI	logical.name
Affected Items > Matching CI Count	matching.ci.count
Title	brief.description
Description	description
Root Cause Description	root.cause
Known Error Detail > Category	incident.category
Known Error Detail > Area	subcategory
Known Error Detail > Sub-area	product.type
Known Error Detail > Impact	initial.impact
Known Error Detail > Urgency	severity
Known Error Detail > Priority	priority.code
Known Error Detail > Solution Identified Date	solutionDate
Known Error Detail > Known Error Resolution Date	expected.resolution.time

Table B-4 Important fields in the knownerror table (cont'd)

Label	Field Name
Known Error Detail > Related Interaction Count	interaction.count
Known Error Detail > Closure Code	closure.code
Known Error Detail > Workaround	workaround
Known Error Detail > Solution	resolution
Assessment > Estimated # of Mandays	estimatedMandays
Assessment > Estimated Costs	estimatedCost
Assessment > Matching configuration Item List	matching.ci

Change Management application tables and fields

Most fields important for the Change Management application are located in the cm3r table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the cm3r table.

Table B-5 Important fields in the cm3r table

Label	Field Name
Change ID	number
Phase	current.phase
Status	status
Approval Status	approval.status
Initiator > Initiated by	requested.by
Initiator > Full Name	full.name
Initiator > Telephone	contact.phone
Initiator > Email	email
Assignment > Assignment Group	assign.dept

Table B-5 Important fields in the cm3r table (cont'd)

Label	Field Name
Assignment > Change Coordinator	coordinator
Affected CI > Service	affected.item
Affected CI > Affected CI	assets
Location	location.full.name
Title	brief.description
Description	description
Change Detail > Category	category
Change Detail > Emergency Change	emergency
Change Detail > Release Management	releaseCandidate
Change Detail > Impact	initial.impact

Configuration Management application tables and fields

Most fields important for the Configuration Management application are located in the device table. The label on the form may not always match the field name in the table. This table associates the label and the field name in the device table.

Table B-6 Important fields in the device table

Label	Field Name
CI Identifier	id
CI Name	logical.name
Asset Tag	asset.tag
Status	istatus
Assignments > Owner	owner
Assignments > Config admin group	assignment
Assignments > Support Groups	support.groups
Assignments > Support Remarks	support.remarks
Assignments > Part Number	part.no

Table B-6 Important fields in the device table (cont'd)

Label	Field Name
Model > Manufacturer	manufacturer
Model > Model	model
Model > Version	version
Model > Serial Number	serial.no
Model > Title	title
Model > Description	comments
Classification > CI Type	type
Classification > CI Subtype	subtype
Classification > Environment	environment
Classification > Security classification	securityClassification
Classification > SOX classification	soxClassification
Classification > Export control classification	expcClassification
Classification > Critical CI	device.severity
Classification > Priority	problem.priority
Classification > Default Impact	default.impact
Classification > User Base	useBase
Classification > System Down	is.down
Classification > Pending Change	pending.change
Classification > Allow Subscribe	allow.subscription
Baseline > Baseline	baseline
Baseline > Baseline Version	baseline.version
Audit > Audit policy	auditPolicy
Audit ->Audit status	auditStatus
Audit > Audit discrepancy	auditDescrepency
Audit > Last audit date	auditDate
Audit > next scheduled audit	scheduledAudit
Audit > Last audited by	auditBy

Index

E

F

I

K

M

N

O

P

R

S

T

U

W