

HP Service Manager – Process Designer Content Pack

For the for supported Windows® and UNIX® operating systems

Software Version: 9.30.3

Processes and Best Practices Guide

Document Release Date: June, 2013

Software Release Date: June, 2013



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 Notice

© Copyright 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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:

<http://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

Contents

Contents	5
Introduction	9
Change Management Overview	10
Change Management within the ITIL framework	10
Change Management application	11
Differences between Change Management and Request Management	11
Change Management process overview	11
Change categories and phases	12
Change Management categories	13
Change Management phases	13
Change Management tasks	14
Change Task phases	14
Change Management user roles	16
Input and output for Change Management	18
Key performance indicators for Change Management	19
ITIL V3 Key Performance Indicators	20
COBIT 4.1 Key Performance Indicators	20
RACI matrix for Change Management	21
Change Management Workflows	26
Register RFC (process ST 2.1)	26
Standard Change (process ST 2.2)	29
Normal Change (process ST 2.3)	31
Emergency Change (process ST 2.4)	37
Review and Close Change (process ST 2.5)	42
Change Management Details	45
Change Management form after escalation from a problem	46
Change Management form details	47
Service Desk Overview	54
Service Desk within the ITIL framework	54
Service Desk application	55

Service Desk process overview	55
Interaction categories	58
Interaction phases	58
Service Desk user roles	59
Input and output for Service Desk Interaction Management	60
Key performance indicators for Service Desk Interaction Management	61
ITIL V3 Key Performance Indicators	61
COBIT 4.1 Key Performance Indicators	62
RACI matrix for Service Desk Interaction Management	62
Service Desk Workflows	63
Self-Service by User (process SO 0.1)	64
Interaction Handling (process SO 0.2)	68
Interaction Matching and Escalation (process SO 0.3)	72
Interaction Closure (process SO 0.4)	75
Withdraw Interaction (process SO 0.5)	79
Service Desk Details	81
New interaction form	82
Interaction form after escalation	83
Service Desk Interaction Management form details	84
Interaction categories	95
Escalate Interaction solution matching	97
Incident Management Overview	98
Incident Management within the ITIL framework	98
Incident Management application	99
Notes for Incident Management implementation	99
Incident Closure process	99
Incident information	99
Incident Management process overview	100
Incident Management categories	101
Incident Management phases	102
Incident Management tasks	103

Incident Task phases	103
Incident Management user roles	103
Input and output for Incident Management	105
Key performance indicators for Incident Management	105
ITIL V3 Key Performance Indicators	106
COBIT 4.1 Key Performance Indicators	106
RACI matrix for Incident Management	108
Incident Management Workflows	109
Incident Logging and Categorization (process SO 2.1)	110
Incident Assignment (process SO 2.2)	113
Incident Investigation and Diagnosis (process SO 2.3)	117
Incident Resolution and Recovery (process SO 2.4)	121
Incident Review and Closure (process SO 2.5)	124
Incident Escalation (process SO 2.6)	126
SLA Monitoring (process SO 2.7)	131
OLA and UC Monitoring (process SO 2.8)	134
Complaint Handling (process SO 2.9)	137
Incident Management Details	141
Incident form after escalation from Service Desk	141
Categorize incident form	143
Investigate incident form	143
Recover incident form	144
Review incident form	145
Incident Management form details	146
Problem Management Overview	158
Problem Management within the ITIL framework	158
Differences between Problem Management and Incident Management	159
The Problem Management application	159
Problem Management workflows and categories	159
Problem tasks	160
Problem Management alerts	160

Problem management process overview	160
Problem management phases	162
Problem Management user roles	162
Input and output of Problem Management	164
Key Performance Indicators for Problem Management	166
ITIL V3 Key Performance Indicators	167
COBIT 4.1 Key Performance Indicators	167
RACI matrix for Problem Management	168
Problem Management Workflows	169
Problem Detection, Logging, and Categorization (process SO 4.1)	170
Problem Investigation and Diagnosis (process SO 4.2)	174
Problem Resolution (process SO 4.3)	180
Problem Review and Closure (process SO 4.4)	185
Problem Monitoring (process SO 4.5)	190
Problem Management Details	193
Problem form after escalation from incident	193
Problem form details	195

Chapter 1

Introduction

This document describes best practices with major sections originating from the Service Manager Best Practices guide but with adaptations made to match the new process flows delivered with Process Designer Content Pack 9.30.3. The Process Designer content release reworked previous out-of-the-box flows and delivered new ITIL-v3 aligned flows for the modules including Change Management, Service Desk, Incident Management, and Problem Management.

Chapter 2

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's infrastructure. This includes assets such as network environment, facilities, telephony, and resources. Change Management enables you to control the changes to baseline service assets and configuration items across the entire service lifecycle.

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 application
- Change Management process overview
- Input and output for Change Management
- Key performance indicators for Change Management
- RACI matrix for Change Management

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).
- Minimize overall business risk.
- Respond to customers' changing business requirements, maximize value and reduce the number of 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 follow to handle a change
- The order in which the steps are to be followed
- Roles and responsibility of the stakeholders
- Scheduling and planning
- When and how to escalate a change

Change Management application

The primary objective of Change Management is to enable beneficial changes to be made with minimal disruption to IT Services. Changes are recorded, 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 change management concepts of ITIL to ensure that the best practices of IT service management are applied to the application.

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 a managed configuration item in most business infrastructures. However, the network password someone uses to log into that PC is not 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

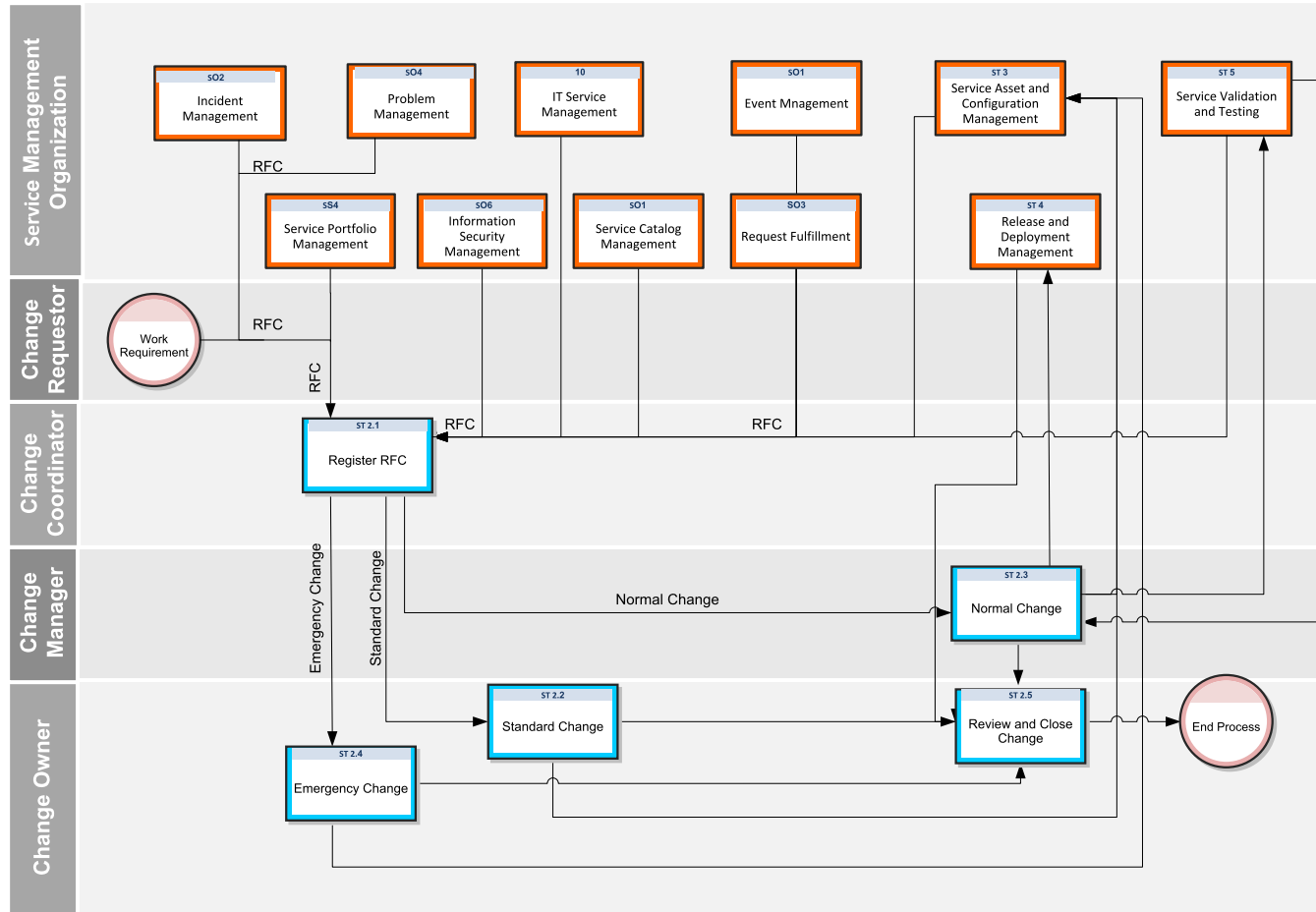
The Change Management process includes the activities necessary to control changes to service assets and configuration items across the entire service lifecycle. It provides standard methods and procedures to use when implementing all changes.

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 throughout a simple or complex lifecycle.

The following figure is the process diagram for Change Management. For more information, see section "[Change Management Workflows](#)" on page 26.



Change categories and phases

Change Management uses categories to 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.

The new best practice process flows shipped with the Process Designer Content Pack introduce three new ITIL v3 aligned process flows for Standard, Normal, and Emergency changes. These correspond to the “Standard Change”, “Normal Change”, and “Emergency Change” categories. This is a change with previous releases of Service Manager where at the category-level more specific changes were classified, such as Hardware or Software. In a system that applies Process Designer Content Pack, they are added to any preexisting categories including any prior OOB categories that may still exist in the system.

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

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 has a change category and phase, but tasks are optional.

Service Manager provides three out-of-box categories you can use to classify the changes in your business. The following table describes the out-of-box Change Management categories.

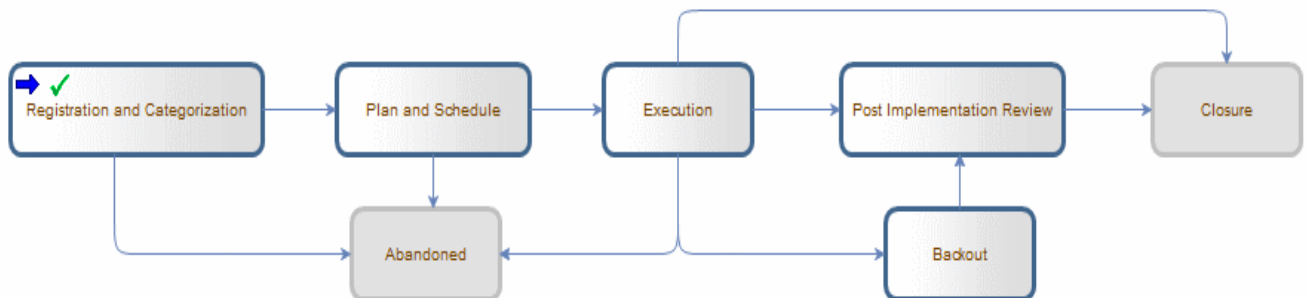
Change Management categories

Category	Description
Emergency Change	Emergency changes are the change processes to be applied in the production environment during emergency situations like service outage.
Normal Change	Normal Change is a change that is categorized, prioritized, planned and that follows all approvals before deployment. Normal Change can be further categorized as Major RFC and Minor RFC.
Standard Change	A Standard Change is a preapproved Change that is of low risk, relatively common and follows a standard procedure.

Change Management phases

Service Manager uses phases to describe the steps needed to complete a change request. The phase also determines the change screens users see, the approvals required to advance to the next phase, and the conditions that cause the system to issue alerts.

For example, the following figure shows the workflow phases for a Standard Change.



Change Management tasks

Service Manager lists the change tasks necessary to complete a particular phase. Workflow cannot proceed to the next phase until all the associated tasks of the current phase are completed. Tasks can be either sequential or parallel. For example, suppose you are in the Deployment phase of a normal change, to replace a hard drive. The change tasks listed may be to take a backup of the old hard drive, remove the old drive, install a new hard drive, test the new hard drive, and restore the data on to the new hard drive. In this example, the tasks are sequential because you cannot restore data onto a new drive until you take a backup of the data and install the new hard drive. Parallel tasks might include determining the backup software to be used, the hard drive vendor to purchase from, and the effort and risk the hard drive change might bring forth. Each phase can optionally have one task / multiple tasks / no tasks. Tasks include a description, the urgency and priority of the task, task scheduling, and assignment information.

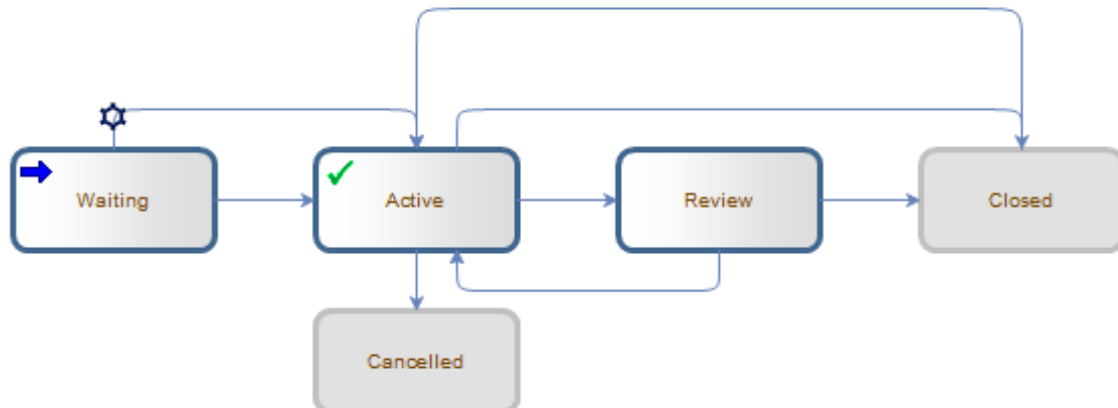
Change Management tasks include:

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

Change Task phases

This section describes the flow of a change task as it progresses from the 'Waiting' phase to the 'Closed' phase in the Generic Task workflow. This workflow is required to implement task dependencies.

The following figure shows the Generic Task workflow in Process Designer.



To change the phases of a change task in the Generic Task workflow:

1. Log on as a Change Coordinator, and then search for an open change request.
2. Click **More > Open New Task** from the menu to create a new change task.

Or

Click the task number in the **Tasks** section to open an existing change task.
3. When a task is opened, it is in the 'Waiting' phase. When the task is being executed, it is in the '**Active**' phase. The Change Implementer (assignee) changes the status of task from '**Ready**' to '**Assigned**' and then to '**In Progress**'. Task status is changed to '**Completed**' when the task is accomplished.
4. If the Change task is not planned to be implemented or if it is not successful, select the task status '**Cancelled**' and the task will be moved to '**Cancelled**' phase.
5. Change task can be closed directly from 'Active' phase bypassing the '**Review**' Phase.
 - If the Risk Assessment value of the change task is less than or equal to 2, then the **Review** phase is bypassed.
 - If the Risk Assessment value of the change task is more than 2 (for example 3 or more), task enters the **Review** phase.
6. Login as Change Reviewer, retrieve the task, and review it. Type your comments in the **Review Comments** field.
7. If the task completed is acceptable, close the task by selecting Successful from the **Closure Code** dropdown list and add closure comments, the task is now in the '**Closed**' phase. If the task is not completed and needs to be reworked, click **Reopen** after adding review comments. The task moves back to the previous '**Active**' phase and to the '**Assigned**' status.
8. Repeat the same steps from 2 to 7 if you want to create, implement and close the tasks at any phase of the change request.
9. A notification is sent to Change Owner on the successful completion of task.

Change Task Status value and display list mapping is as follows:

Value	Status
0	Planned
1	Ready
2	Assigned
3	In Progress
4	Blocked
20	Completed

Value	Status
21	Completed with Problems
30	Cancelled
31	Withdrawn
32	Failed

Change Management user roles

The following table describes the responsibilities of the Change Management roles.

Change Management user roles

Role	Responsibilities
Change Approver	<ul style="list-style-type: none"> • Uses the Service Management tool or Change Advisory Board to approve or deny Change when requested. • Facilitates Emergency Change Advisory Board (E-CAB) meetings.
Change Coordinator	<ul style="list-style-type: none"> • 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 Risk and Impact Analysis phase of the change and creates change plan based on the assessment information. • Verifies if the change has passed the test criteria. • Verifies if the change is implemented successfully in the production environment. • After implementation, evaluates the change and closes the request. • If a change implementation fails, the coordinator activates a back-out plan to return the system to its original state.

Change Management user roles, continued

Role	Responsibilities
Change Owner	<ul style="list-style-type: none"> • Assesses the validity of the RFC and involves in risk assessment. • Performs post implementation review and responsible for closure of change. • Responsible for convening the ECAB members for Emergency Change approval. • Coordinates with the experts within change process for Build and Test activities. Reviews, revises, and updates schedule for Emergency and Standard Changes. • Plans, receives, and reviews RFC for approvals. • Generates CMDB updates to be submitted to Service Asset and Configuration Management for processing.
Change Manager	<ul style="list-style-type: none"> • Reviews all changes after the Plan and Schedule phases and forwards them to the right Change Approver. • Organizes Change Advisory Board meeting if necessary. • Updates the change after approval. • Periodically reviews changes in a Post Implementation Review; determines and executes follow-up actions. • Coordinates all activities in case the Emergency Change Handling process is triggered.
ECAB	<ul style="list-style-type: none"> • Validates that the Emergency Change is truly an emergency (based on emergency change criteria). • Ensures the RFC for Emergency Change is complete. • Ensures the RFC for Emergency Change receives appropriate approval (based on the Change Management Policy). • Makes the final decision that the resolution being implemented to correct the production issue is the best option for the situation. • Ensures the Emergency Change is reviewed by the CAB, post implementation.

Change Management user roles, continued

Role	Responsibilities
Technical Change Advisory Board (TCAB)	<ul style="list-style-type: none">• Responsible for analyzing and reviewing the risk and impact of change request.• Authorizes, disapproves, or requests more information for each Normal Major change request.• Ensures all Normal Major changes are adequately assessed and prioritized.• When requested, participates in Change Post Implementation Reviews.
Deployment Change Advisory Board (DCAB)	<ul style="list-style-type: none">• Reviews the Build and Test results and approves, abandons, or rejects them. If the Build and Test results are approved, the DCAB reviews and updates the implementation schedule and authorizes the Normal Change implementation to begin.• Participates in scheduling and coordination of the change.• When requested, participates in Change Post Implementation Reviews.

Input and output for Change Management

Changes can be triggered and resolved in several ways. The following table outlines the input and output for the Change Management process.

Input and output for Change Management process

Input to Change Management	Output from Change
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 the following table are useful for evaluating a Change.

Key Performance Indicators for Change Management

Title	Description
% of unauthorized changes	Percentage of unauthorized implemented changes in a given 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 period.
% of emergency changes	Percentage of the total number of closed emergency changes in a given period.
% of successful changes	Percentage of the total number of closed changes successfully implemented in a given period.
% of backed out changes	Percentage of the total number of closed changes for which a remedy plan is activated in a given period.
% of rejected changes	Percentage of the total number of closed changes rejected in a given period.

Key Performance Indicators for Change Management, continued

Title	Description
Average time per phase	Average amount of time spent on each of the distinct change phases in a given period. Validation, Risk and Impact Analysis, TCAB Approval, Build and Test, DCAB Approval, Deployment, Post Implementation Review, CMDB Update, and Closure.

For completeness, the ITIL V3 and COBIT 4.1 KPIs are included in the following sections.

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 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 to the costs of the change process.
- Reduction in the number of disruptions to services, defects, 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.
- Extent of application rework caused by inadequate change specifications.
- Minimum time and effort required to make changes.
- Percentage of emergency fixes.
- Percentage 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.
- Percentage of changes recorded and tracked with automated tools.
- Percentage of changes that follow formal change control processes.
- Ratio of accepted and 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 the following table.

RACI matrix for Change Management

Process ID	Activity	Change Manager	Change Requestor	Change Coordinator	Change Advisory Board (CAB)	Change Approver (or ECAB)	Change Owner
ST 2.1	Register RFC	A	R	R			

RACI matrix for Change Management, continued

Process ID	Activity	Change Manager	Change Requestor	Change Coordinator	Change Advisory Board (CAB)	Change Approver (or ECAB)	Change Owner
ST 2.1.3	Perform RFC Assessment	A	I	R		C/I	
ST 2.1.5	Reject RFC	C/I	R	R	R		
ST 2.1.6	Assign Change Owner	R	R	R			
ST 2.2.1	Identify Standard Change Model and Change Owner	R/A	R	I			I
ST 2.2.2	Prioritize Standard Change	R/A	C/I	I			R
ST 2.2.3	Plan and Schedule Standard Change	R/A	I	R			R
ST 2.2.4	Execute Standard Change	R/A	I	R			R
ST 2.2.6	Remove Standard Change Model	R	I	I			C/I
ST 2.3.1	Assess Change	R/C	I	R			R
ST 2.3.3	Determine Approval Requirements	R	C/I	C/I			A

RACI matrix for Change Management, continued

Process ID	Activity	Change Manager	Change Requestor	Change Coordinator	Change Advisory Board (CAB)	Change Approver (or ECAB)	Change Owner
ST 2.3.5	TCAB Approval	R/A	I	I	R		
ST 2.3.8	Coordinate Build and Test	R.A	I	R			R
ST 2.3.10	Schedule for Normal Change	R/A	I	R			R
ST 2.3.12	Create and Submit Deployment Plan	A	I	R			R
ST 2.3.13	DCAB Approval	R/A	I	I	R		
ST 2.3.15	Decision on Rebuild	R/A			R		
ST 2.3.17	Review RFC after Rebuild Decision	A	I	R			R
ST 2.3.19	Review RFC after DCAB Approval	A	I	R			R
ST 2.3.21	Coordinate and Monitor Change Implementation	R/A	I	R/C			R
ST 2.3.23	Provide CMDB Updates	R/A	I	R			R
ST 2.3.26	Assess Change Success	R/A	I	R			R

RACI matrix for Change Management, continued

Process ID	Activity	Change Manager	Change Requestor	Change Coordinator	Change Advisory Board (CAB)	Change Approver (or ECAB)	Change Owner
ST 2.4	Emergency Change	R/A	C/I		R	R	R
ST 2.4.3	Convene ECAB	R/A				C/I	R
ST 2.4.4	Approve Emergency Change	A/C				R	
ST 2.4.6	Plan and Design Solution	R/A		I			R
ST 2.4.8	Coordinate Emergency Change Build and Test	R/A	I	R			R
ST 2.4.10	Coordinate Emergency Change Implementation	R/A					R
ST 2.4.11	Abandon the Change	R	C	I			R
ST 2.5	Review and Close Change	R/A	C	R			R/C
ST 2.5.3	Conduct Formal Turnover to Support	C/I	C	A/C			R
ST 2.5.4	Perform PIR	A	C/I	R			R

RACI matrix for Change Management, continued

Process ID	Activity	Change Manager	Change Requestor	Change Coordinator	Change Advisory Board (CAB)	Change Approver (or ECAB)	Change Owner
ST 2.5.5	Notify Requestor of Change Results	A/C	I	R			R
ST 2.5.6	Close RFC	R/A	C	R			R

Chapter 3

Change Management Workflows

Change Management controls the process to request, manage, approve, and control changes that modify your organization's 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, E-mail, and phone calls.

Note: All three change workflows (Standard, Normal, and Emergency) have an implementation phase but each are named differently: Execution, Deployment, and Implementation respectively. The names are by design and selected to match the types of activities for the flows as specified in ITIL v3. Because the activities are not same, the implementation phase in each workflow is named differently.

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

Note: The following processes are depicted with a light blue border in each of the workflow diagrams in the following section.

- Register RFC (process ST 2.1)
- Standard Change (process ST 2.2)
- Normal Change (process ST 2.3)
- Emergency Change (process ST 2.4)
- Change Review and Close Change (process ST 2.5)

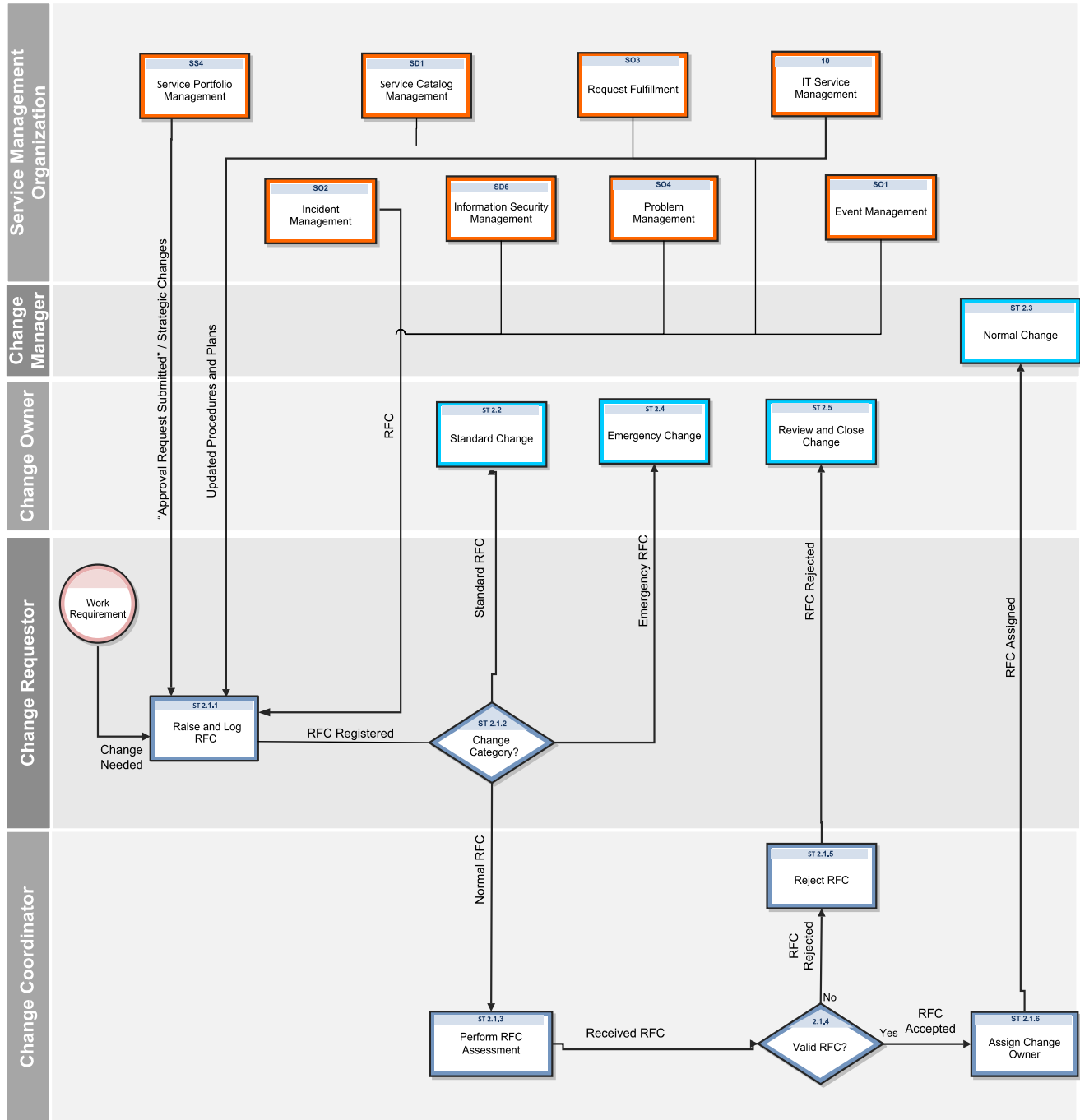
Register RFC (process ST 2.1)

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, and Problem Management. Each RFC must be registered in an identifiable way. HP Service Manager provides change templates that standardize and speed up the Change Registration process. RFCs are received from requestors. In some cases, RFCs are logged on the requestor's behalf. For example, a business unit may require additional facilities. Another scenario may be that the Problem Management staff initiates solution for an error from several other sources. All RFCs are reviewed for completeness and accuracy. There may be additional information that must be entered into the RFC log prior to further processing.

The following user roles can perform Change Registration:

- Change Requestor
- Change Coordinator

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



Register RFC process

Process ID	Procedure or Decision	Description	Role
ST 2.1.1	Raise and Log RFC	All RFCs received are logged, provided with a unique identification number. Any other relevant information about the change request is also recorded. If the change request is in response to a trigger, i.e., a resolution to a Problem Record (PR), then the reference number of the triggering document is retained for traceability. The change is categorized (Standard, Normal, or Emergency) at the time of logging.	Change Requestor
ST 2.1.2	Change Category?	If this is a Standard Change, it will follow the Standard Change processes. If this is a Normal Change, it will follow the Normal Change processes. If this is an Emergency Change, it will follow the Emergency Change processes.	Change Requestor
ST 2.1.3	Perform RFC Assessment	The Change Coordinator receives the RFC and assesses it to determine whether it is valid. The RFC is rejected if: <ul style="list-style-type: none"> • The RFC is impractical • The RFC is a duplicate <p>Note: The activities of logging and categorizing an RFC may be delegated to a Change Coordinator if desired.</p>	Change Coordinator
ST 2.1.4	Valid RFC?	The Change Coordinator determines whether the RFC is valid.	Change Coordinator
ST 2.1.5	Reject RFC	The Change Coordinator updates the RFC with an explanation of the rejection, and notifies the requestor.	Change Coordinator
ST 2.1.6	Assign Change Owner	The Change Coordinator looks for resources and assigns a Change Owner.	Change Coordinator

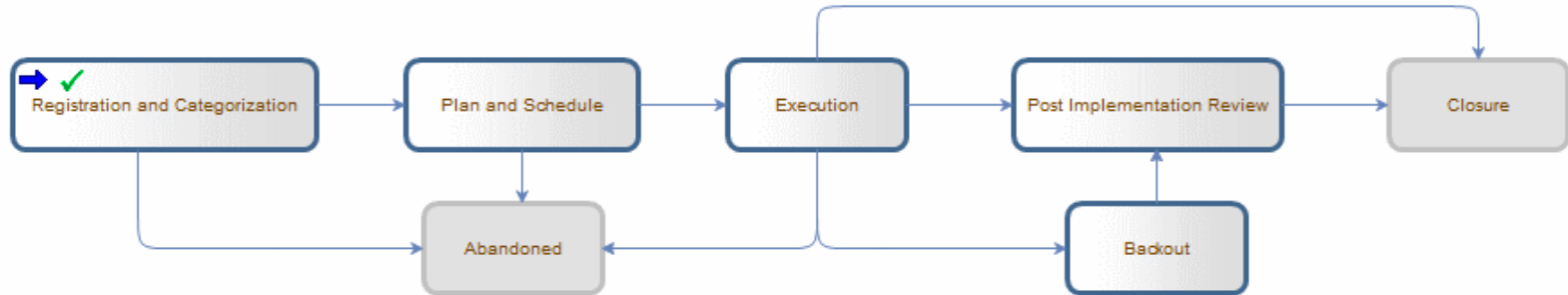
Standard Change (process ST 2.2)

A Standard Change is a preapproved change that follows a standard procedure; for example, a password reset or the provision of standard equipment to a new employee. Standard Change uses the Change Model configured in the system which can pre-populate the information in the Change ticket on registering the Change.

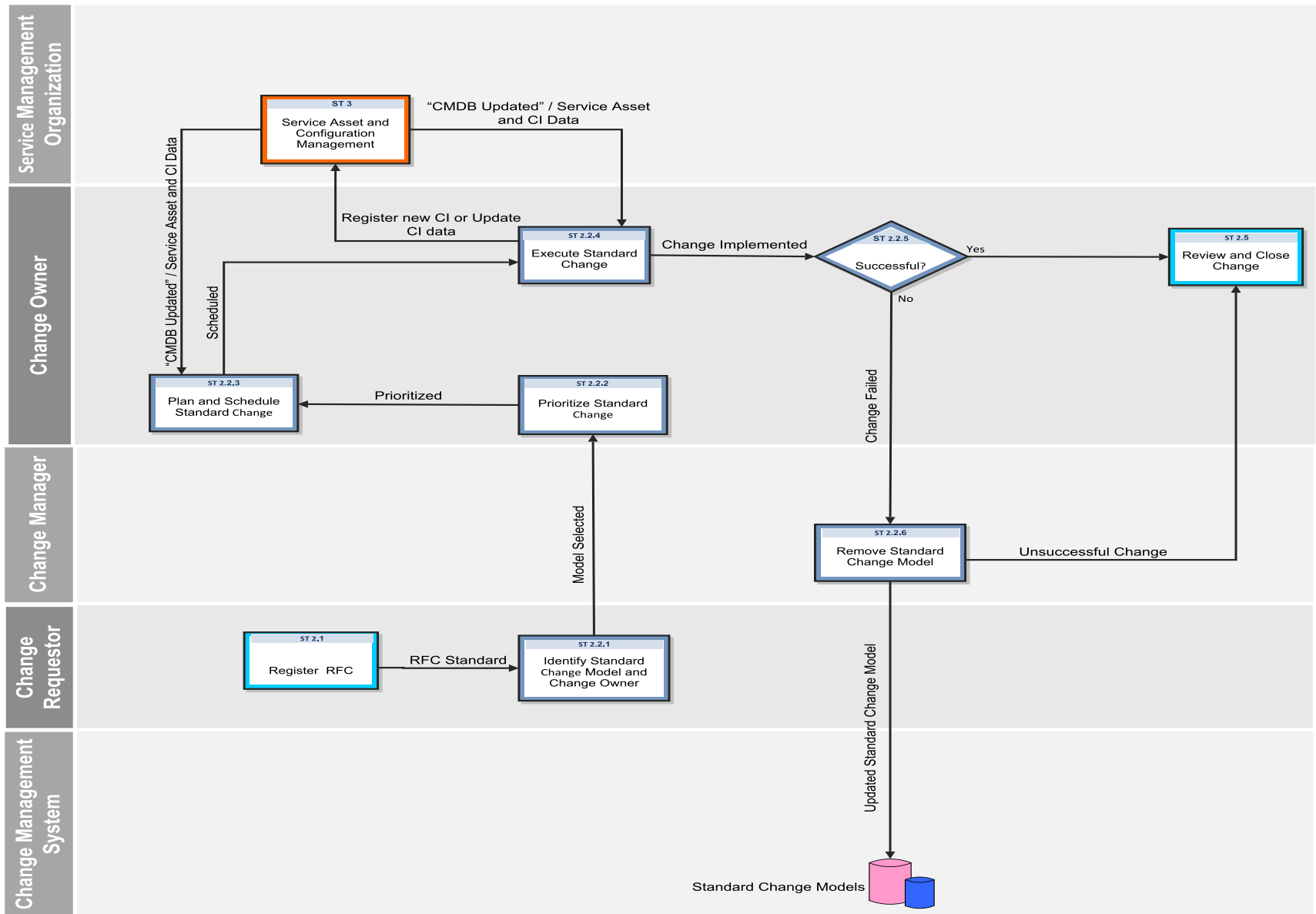
For an activity to be accepted as a Standard Change, the following requirements must be met:

- The documented tasks must be commonly known and proven
- Authority will be given in advance based on predetermined criteria
- The chain of events can be initiated by a functional Service Desk
- Budgetary approval will typically be predetermined or within the control of the Change Requestor

The following figure depicts the Standard Change workflow in Process Designer.



For details of the Standard Change process, see the following figure and table.



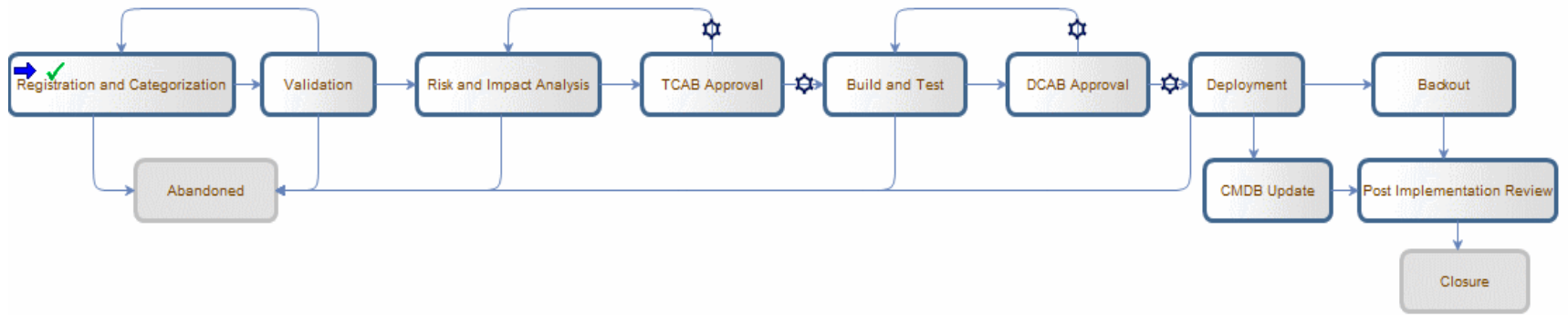
Standard Change process

Process ID	Procedure or Decision	Description	Role
ST 2.1	Register RFC	RFCs are logged by the Change Requestors. All RFCs are reviewed for completeness and accuracy.	Change Requestor
ST 2.2.1	Identify Standard Change Model and Change Owner	The Standard change model that has to be requested is first identified and then the Change Owner is decided. In many cases the change owner is documented with the change model. If this is not the case, a Change Owner is decided manually.	Change Requestor
ST 2.2.2	Prioritize Standard Change	Standard change is prioritized as High, Medium, or Low depending on the impact and urgency.	Change Owner
ST 2.2.3	Plan and Schedule Standard Change	The Change Owner plans the resources required, and also reviews revises and updates the schedule for Standard Changes as needed.	Change Owner
ST 2.2.4	Execute Standard Change	The Change Owner executes the Standard Change. The CMDB is updated according to the changes performed.	Change Owner
ST 2.2.5	Successful?	The Change Owner checks whether the Change is successful.	Change Owner
ST 2.2.6	Remove Standard Change Model	If a Change Implementation is unsuccessful, the Standard Change Model may need to be slightly modified or removed from the database.	Change Manager
ST 2.5	Review and Close Change	The Change Owner reviews the change implementation and closes it if successful.	Change Owner

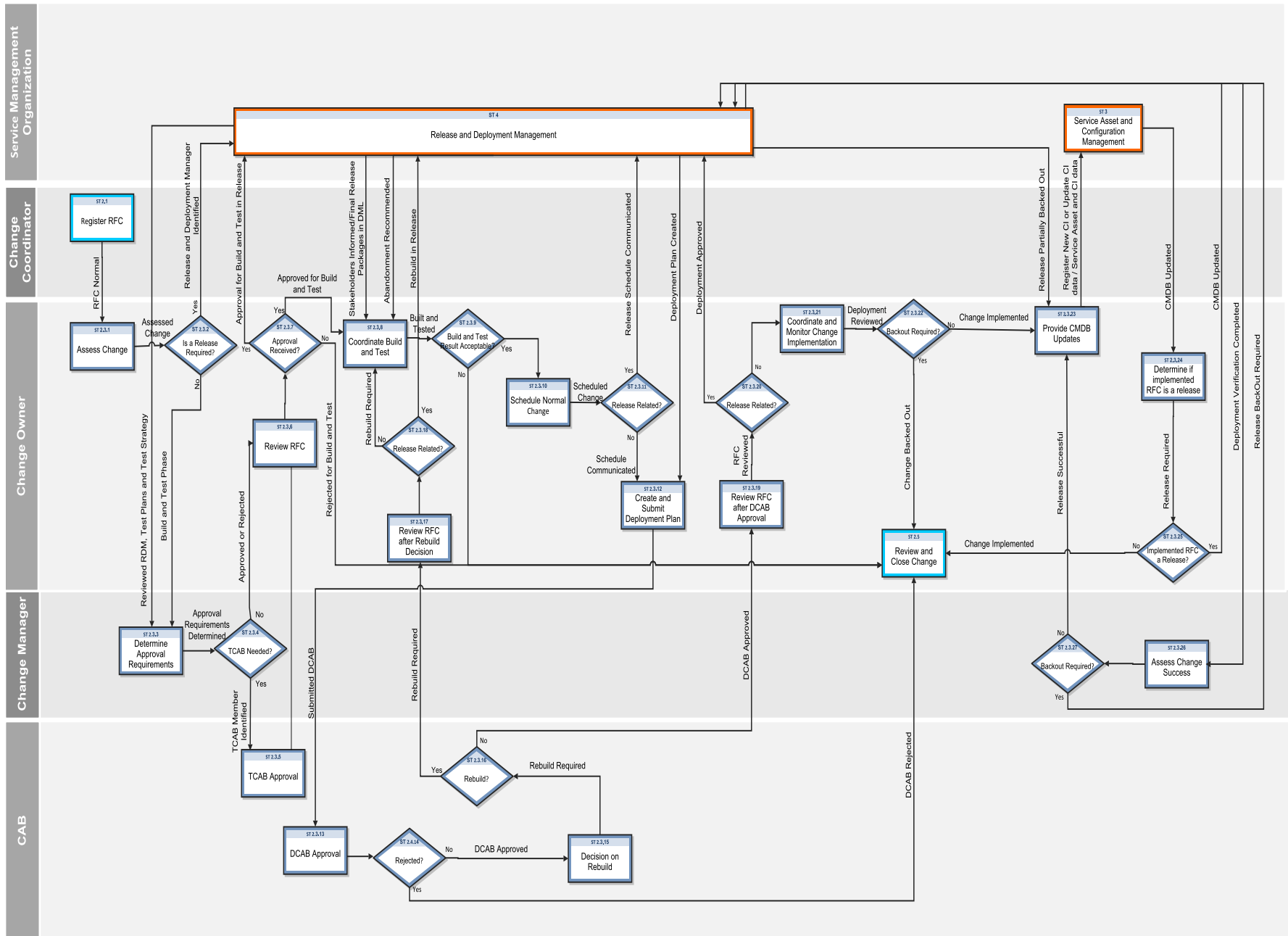
Normal Change (process ST 2.3)

Normal Change is a change that is categorized, prioritized, planned and that follows all approvals before deployment. The Normal Change activities describe the steps necessary to process a Normal Change by coordinating work effort. Normal Change can be further categorized as Major and Minor. Both Major and Minor changes go through the same workflow except that, for a Normal Major RFC the TCAB Approval phase is a manual transition & the change has to be approved manually by TCAB members. In a Normal Minor RFC the TCAB Approval phase is auto approved, this phase is optional in Minor RFC but it is still configured in Out of Box. The Change must be appropriately reviewed, approved, and executed successfully through the Normal Change process at least once prior to acceptance.

The following figure depicts the Normal Change workflow in Process Designer.



For details of the Normal Change process, see the following figure and table.



Normal Change process

Process ID	Procedure or Decision	Description	Role
ST 2.1	Register RFC	RFCs are logged by the Change Requestors. All RFCs are reviewed for completeness and accuracy.	Change Coordinator
ST 2.3.1	Assess Change	Assessing a change includes determining the risk and impact and identifying if the change requires a release to be generated. If a release is required, a Release and Deployment Manager is identified.	Change Owner
ST 2.3.2	Is a Release Required?	The Change Owner determines whether a release is required to implement the change.	Change Owner
ST 2.3.3	Determine Approval Requirements	The Change Manager reviews the change and decides whether a TCAB needs to be convened.	Change Manager
ST 2.3.4	TCAB Needed?	If TCAB is not needed, the Change Manager determines whether the change should be approved or rejected. If TCAB is needed, members are identified and change is submitted for approval.	Change Manager
ST 2.3.5	TCAB Approval	Change Manager works with TCAB and approves the Change.	CAB
ST 2.3.6	Review RFC	The Change Owner reviews the RFC for approvals.	Change Owner
ST 2.3.7	Approval Received?	Upon approvals, build and test is performed either by Release and Deployment process or Change Management process. If unapproved, the RFC is closed.	Change Owner

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
ST 2.3.8	Coordinate Build and Test	<p>The Change Owner initiates the Release and Deployment Management process to perform build and test. The Service Validation Testing process is involved in validating and testing the build created by release.</p> <p>In case the build and test is unsuccessful, it is recommended to abandon the change to RDM which in turn is informed to the Change Owner.</p> <p>The Change Owner coordinates between the experts within Change process for building and testing activities. The change is built and tested thoroughly and validated.</p>	Change Owner
ST 2.3.9	Build and Test Result Acceptable?	If the Build and Test result is acceptable, deployment is scheduled; else the RFC is sent for closure.	Change Owner
ST 2.3.10	Schedule for Normal Change	Change Owner involves the RDM and prepares the schedule for normal change. This schedule is based on the draft deployment plan obtained from the Release and Deployment Management process received.	Change Owner
ST 2.3.11	Release Related?	If release is related, the detailed deployment plan is created by the RDM process; else, Change Owner creates the same.	Change Owner
ST 2.3.12	Create and Submit Deployment Plan	The Change Owner creates the Deployment plan and submits it to DCAB approval. The same is also received from RDM and is sent for DCAB's review.	Change Owner
ST 2.3.13	DCAB Approval	DCAB reviews the Build and Test results and approves / abandons / rejects as deemed fit. If the Build and Test results are approved, DCAB reviews and updates the implementation schedule and authorizes the Normal Change implementation to commence.	CAB
ST 2.3.14	Rejected?	If DCAB rejects the change, it moves to closure.	CAB
ST 2.3.15	Decision on Rebuild	If DCAB decides on rebuilding, the change is rebuilt and tested again.	CAB

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
ST 2.3.16	Rebuild?	If a rebuild is required, the Change Owner is informed; else, the change is deployed.	CAB
ST 2.3.17	Review RFC after Rebuild Decision	The Change Owner reviews the RFC to check whether the rebuild will be performed by RDM or within change. Also a decision is made on what modules to be rebuilt and the timeline.	Change Owner
ST 2.3.18	Release Related?	If the rebuild is related to RDM, the request is sent to RDM for rebuilding and testing; else, these are performed within Change Management process.	Change Owner
ST 2.3.19	Review RFC after DCAB Approval	The Change Owner reviews the RFC to go ahead with the deployment.	Change Owner
ST 2.3.20	Release Related?	If RDM is involved for deployment, RDM carries out the deployment activities; else it is carried out by the Change Management.	Change Owner
ST 2.3.21	Coordinate and Monitor Change Implementation	The Change Owner coordinates and monitors the Normal Change implementation. Various tasks are created for carrying out the deployment activities as mentioned in the deployment plan. After the deployment, the Change owner verifies whether the deployment was successful or not.	Change Owner
ST 2.3.22	Back Out Required?	If the change is unsuccessful it is backed out and moved to closure; else CMDB is updated for successful changes.	Change Owner
ST 2.3.23	Provide CMDB Updates	Change Owner generates CMDB updates that are to be submitted to Service Asset and Configuration Management for processing.	Change Owner

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
ST 2.3.24	Determine if implemented RFC Is a Release	If the implemented change involves a release, control is returned to Release and Deployment Management for further review and closure.	Change Owner
ST 2.3.25	Implemented RFC for a Release?	If the RFC was for a release, the post-deployment activities will take place in the Release and Deployment Management process; else move on to PIR.	Change Owner
ST 2.3.26	Assess Change Success	The Change Manager determines whether the change implementation is successful.	Change Manager
ST 2.3.27	Back Out Required?	If a release needs to be backed out, this is done in the Release and Deployment Management process.	Change Manager

Emergency Change (process ST 2.4)

Emergency changes can also be initiated in 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:

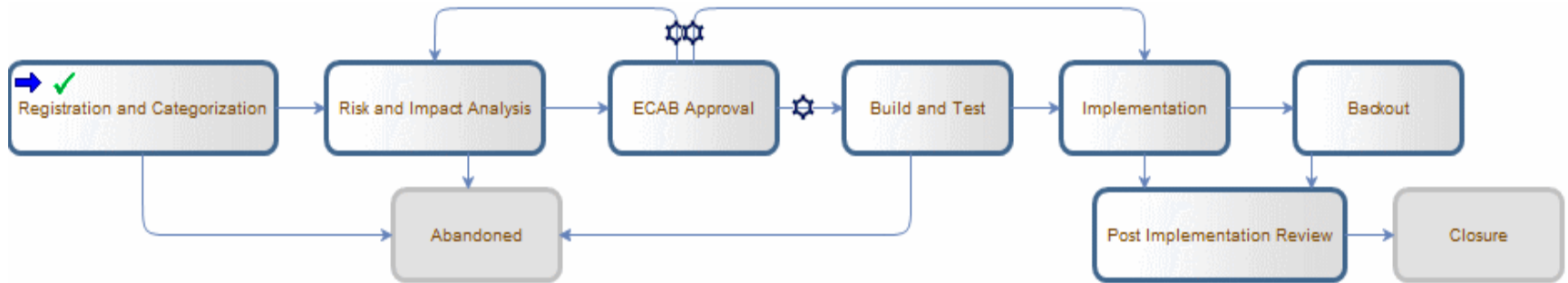
- Approval is given by the Emergency Change Approval Board (E-CAB) instead of waiting for a regular CAB meeting.
- Testing may be reduced, or in extreme cases eliminated, if doing so is considered necessary to deliver the change immediately.
- Updating of the change request and configuration data may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

If the E-CAB decides to handle an emergency change as a normal change, the emergency change is recategorized and implemented using the normal change process.

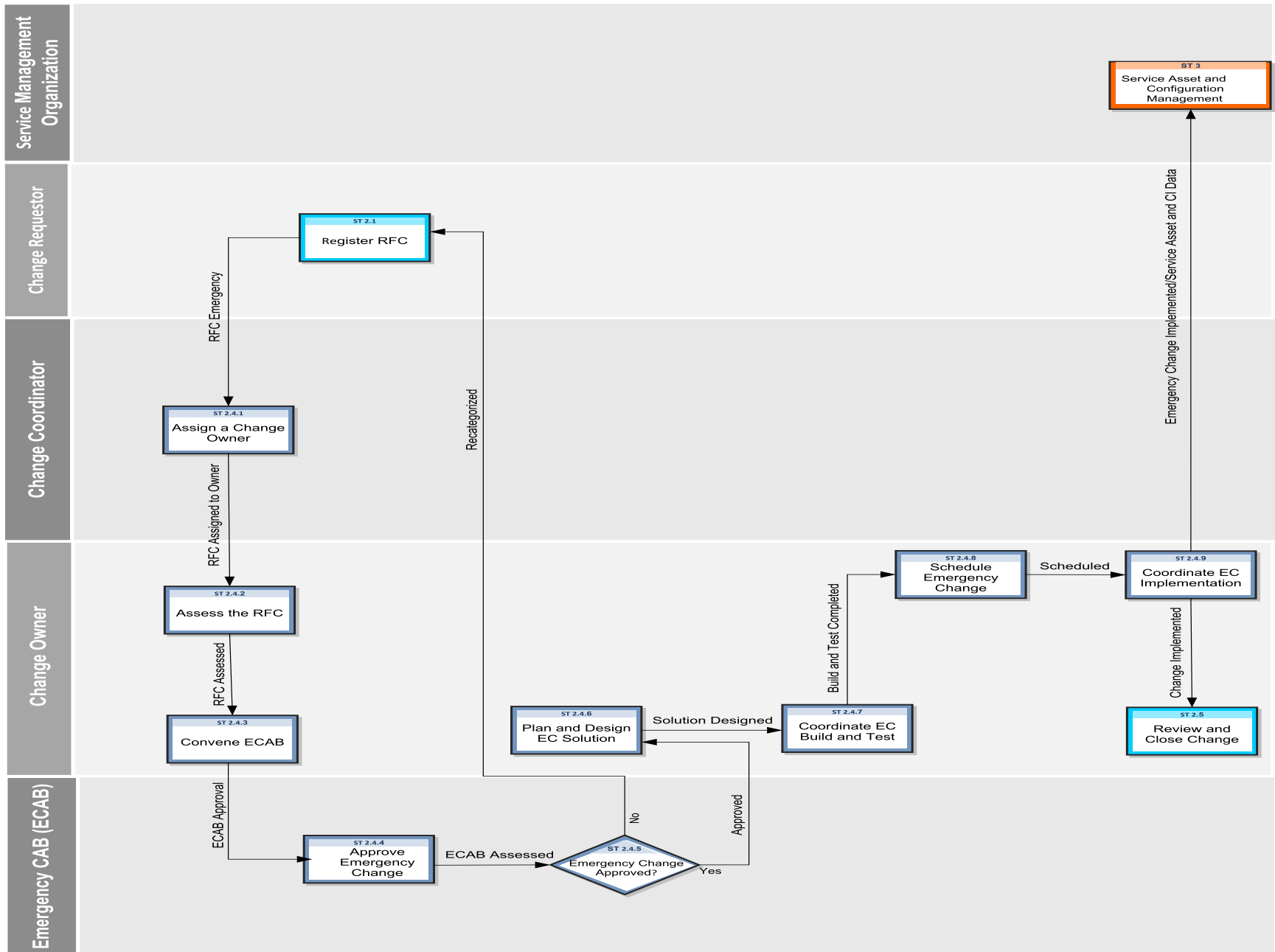
The following user roles are involved in Emergency Change Handling:

- Change Manager
- E-CAB
- Change Owner

The following figure depicts the Emergency Change workflow in Process Designer.



For details of the Emergency Change process, see the following figure and table.



Emergency Change process

Process ID	Procedure or Decision	Description	Role
ST 2.1	Register RFC	Emergency Change activities provide the expedited Change Management process, which implements changes to the production environment due to an emergency occurring by a service outage. RFCs are logged by the Change Requestors.	Change Requestor
ST 2.4.1	Assign a Change Owner	The Change Coordinator assigns the Emergency change to the Change Owner.	Change Coordinator
ST 2.4.2	Assess the RFC	The Change Owner receives the RFC and assesses it to determine whether it is valid. It is re-categorized as Normal if it does not qualify as Emergency Change. Risk and Impact Analysis is done at this stage.	Change Owner
ST 2.4.3	Convene ECAB	The Change Owner convenes Emergency Change Advisory Board (ECAB) members to authorize the change. The E-CAB members are authorized to make decisions about high impact emergency changes.	Change Owner
ST 2.4.4	Approve Emergency Change	ECAB reviews the Emergency Change and assesses its urgency, impact, and risk. Based on their review the ECAB members either approve or deny the change.	Emergency CAB (ECAB)
ST 2.4.5	Emergency Change Approved?	If ECAB approves, the change is implemented. Else the change is denied by the Change Approver and re-categorized as a Normal Change.	Emergency CAB (ECAB)
ST 2.4.6	Plan and Design Solution	The Change Owner plans the resources required, designs the solution to implement Emergency Change.	Change Owner
ST 2.4.7	Build and Test Required?	If Build and Test is required, Change Owner performs the building and testing activities by creating change tasks at this phase of the change. If build and test is not required the change is scheduled for implementation.	Change Owner

Emergency Change process, continued

Process ID	Procedure or Decision	Description	Role
ST 2.4.8	Coordinate Emergency Change Build and Test	The Change Owner coordinates the Build and Test activities for Emergency Change.	Change Owner
ST 2.4.9	Schedule Emergency Change	The Change Owner reviews, revises and updates the schedule as needed for Emergency Change.	Change Owner
ST 2.4.10	Coordinate Emergency Change Implementation	The Change Owner coordinates the activities for implementing the Emergency Change. Successful change implementation is followed by update of the CMDB and formal turnover to support.	Change Owner
ST 2.4.11	Abandon the Change	If an Emergency change is denied by the ECAB, the RFC is abandoned. Go to 2.5 to close the change.	Change Owner
ST 2.5	Review and Close Change	The Change Owner reviews the change implemented and closes if it is successful. Unsuccessful change is backed out and the emergency RFC is closed after PIR (Post Implementation Review). Change tasks are created to roll back the change and to bring the environment to agreed stable state.	Change Owner

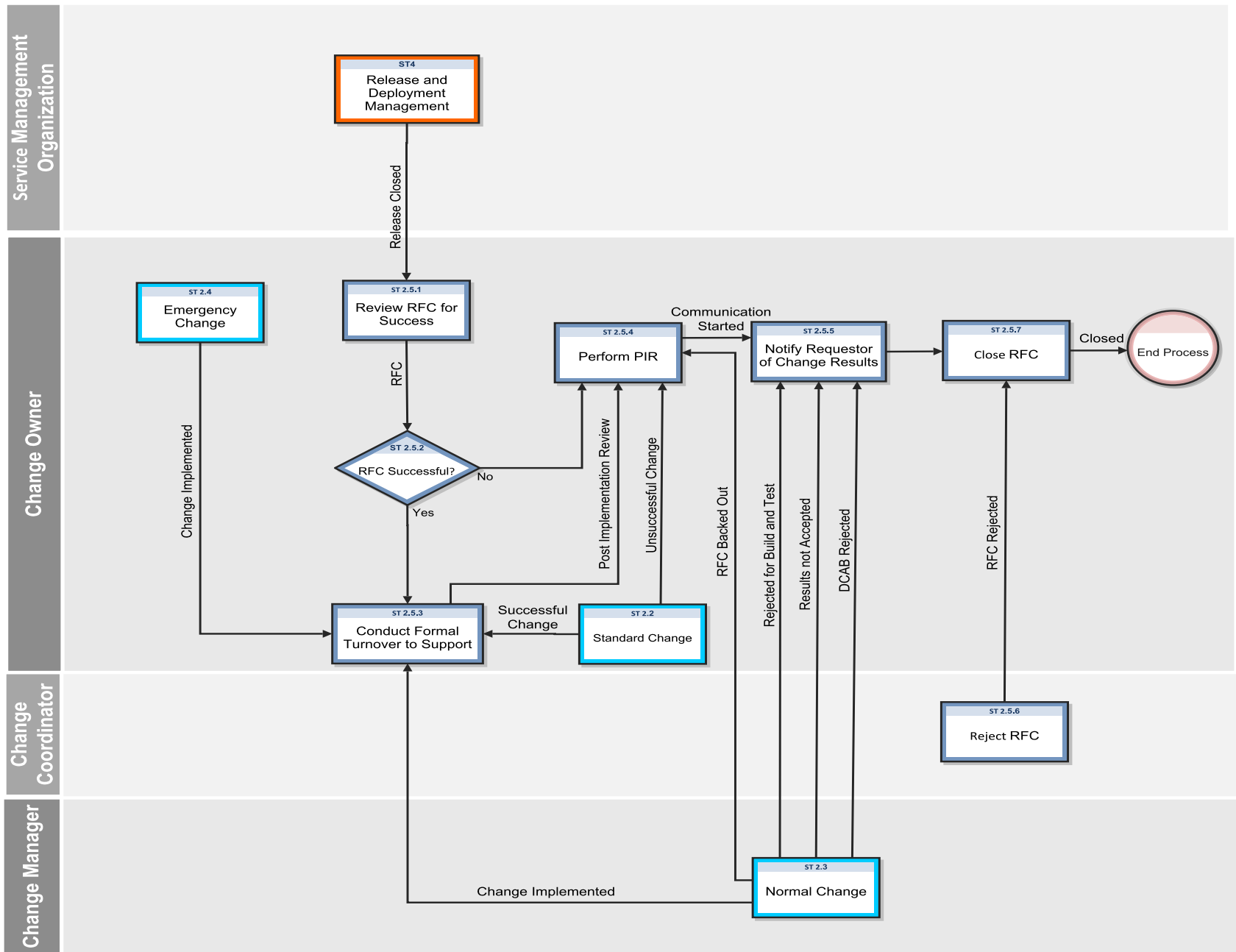
Review and Close Change (process ST 2.5)

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. The Change Owner and Change Manager review the change implementation and close it if successful.

Post-implementation review of the change or PIR) is performed to confirm that:

- The change meets its objectives
- The change Requestor and stakeholders are satisfied with the results
- Unanticipated effects have been avoided.
- Lessons learnt are incorporated in future changes.

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



Review and Close Change process

Process ID	Procedure or Decision	Description	Role
ST 2.5.1	Review RFC for Success	The Change Owner checks whether the RFC deployed by Release and Deployment Management process is successful.	Change Owner
ST 2.5.2	RFC Successful?	If the release is successful, it is handed over to the support staff. If the release is unsuccessful, it is subject to a Post-Implementation Review (PIR).	Change Owner
ST 2.5.3	Conduct Formal Turnover to Support	The Change Owner ensures that all the functionality changes are documented and performs the tasks required to hand over the change to the support staff.	Change Owner
ST 2.5.4	Perform PIR	The Change Owner and Change Manager perform a Post-Implementation Review (PIR) to ensure that the change is reviewed and lessons learned from the change are implemented.	Change Owner
ST 2.5.5	Notify Requestor of Change Results	The Change Requestor is notified of the success or failure of the change.	Change Owner
ST 2.5.6	Close RFC	The Change Requestor is notified of the success or failure of the change.	Change Owner

Chapter 4

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 appropriate approvers and coordinates Emergency Change handling. The Change Approver approves or denies the change request. The Change Coordinator plans the change implementation and verifies if 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 problem
- Change Management form details

Change Management form after escalation from a problem

The following figure shows a new change request escalated from a problem 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 47 for a list and description of the fields on this form.

The following figure is an example of the Change Management form after escalation from a problem.

Change Details

Title *	Memory Upgrade		
Change ID	C10038	Category	Standard Change
Phase	Registration and Categorization	Subcategory	Hardware
Alert Stage		Change Model	Memory Upgrade
Change Requester *	FALCON, JENNIFER	Impact *	4 - User
Requested End Date *	10/12/11 00:38:31	Urgency *	4 - Low
Reason for Change *	Proposed Upgrade	Priority	3 - Average
Service *	Applications	Risk Assessment	1 - Low Risk
Affected Configuration Item		Change Coordinator	
		Change Owner	
		Assignment Group	Hardware
Location		Assignee	
		External Reference	
Description *	Upgrade the memory for workstation or laptop		
Effect of not Implementing *	Upgrade the memory for workstation or laptop		

Change Management form details

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

Change Management field descriptions

Label	Description
Change ID	This is a system-generated field assigned when the change is opened.
Change Model	A change model is a record that is used to predefine the contents of a specific type of Request for Change (RFC), including the information used to populate the RFC and the tasks that are needed to complete the change. When you open a change request using a change model, most of the necessary information is added to the change automatically.
Phase	This is a system-generated field that specifies the name of the current phase of the change.
Approval Status	<p>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.</p> <p>These approval statuses are available out-of-box:</p> <ul style="list-style-type: none"> • Pending • Approved • Denied
Change Requestor	<p>The name of the user requesting the change.</p> <p>This is a required field. This field includes a hover-over form that displays full name, telephone, and email address if available for the user requesting the change.</p>

Change Management field descriptions, continued

Label	Description
Assignment Group	<p>The group assigned to work on the change. For a description of this field see the Assignment Group field description in the Incident Management form details section in the Service Manager Processes and Best Practices Guide as this field functions similarly. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups.</p> <p>You may want to change the sample assignment groups to meet your own needs.</p> <p>These assignment groups are available out-of-box:</p> <ul style="list-style-type: none"> • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager
Change Coordinator	<p>The person responsible for coordinating the change implementation. Each Change Coordinator may belong to several assignment groups. Each group must have only one Change Coordinator.</p>
Service	<p>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.</p> <p>This is a required field.</p>

Change Management field descriptions, continued

Label	Description
Affected CI	The list of Configuration Items (CIs) affected by the change. The system prepopulates this field when a change request is created from an incident or problem. Users can add additional CIs. This field includes a hover-over form that displays check boxes for Critical CI and Pending Change.
Location	Specifies the location for the change. The system prepopulates this field when the change is created by escalating an interaction.
Title	Provides a short description or a gist of the change. This is a required field.
Description	Provides a detailed description of the change. This is a required field.
Category	This is a system-generated field that classifies the type of change.
Emergency Change	<p>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 speed up the process. Emergency changes go directly to the Prepare for Change Approval phase. The system also adds the Emergency Group Approval to the ECAB Approval phase and creates an activity record that shows "This change is logged as an Emergency Change" in the Activities > Historic Activities section.</p> <p>There are notifications to the Change Manager every time there is an activity (open, update or closure of an emergency change).</p>
Impact	<p>This field is prepopulated with data from an incident when a change is created from an incident. It specifies the impact the problem has on the business. The impact and the urgency are used to calculate the priority.</p> <p>These impacts are available out-of-box:</p> <ul style="list-style-type: none"> ● 1 - Enterprise ● 2 - Site/Dept ● 3 - Multiple Users ● 4 - User <p>The out-of-box data is the same as Interaction Management, Problem Management, and Incident Management.</p> <p>This is a required field.</p>

Change Management field descriptions, continued

Label	Description
Urgency	<p>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 more information, see User Interaction Management form details in the Service Manager Processes and Best Practices Guide.</p> <p>This is a required field.</p>
Priority	<p>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 in the Service Manager Processes and Best Practices Guide.</p>
Risk Assessment	<p>Specifies a code that indicates the risk incurred with the implementation of the change. This field becomes required in the Change Plan and Schedule phase.</p> <p>These risk assessments are available out-of-box:</p> <ul style="list-style-type: none"> • 0 - No Risk • 1 - Low Risk • 2 - Some Risk • 3 - Moderate Risk • 4 - High Risk • 5 - Very High Risk <p>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. This is a required field.</p>
Requested End Date	<p>The system prepopulates this field if the change request is created from an interaction escalation. This is the date the change initiator requests the change implementation. This is a required field if not prepopulated.</p>
Alert Stage	<p>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.</p>

Change Management field descriptions, continued

Label	Description
Scheduled Implementation Start	This field specifies the date and time that the work to implement the change should start. This field becomes required in the Plan and Schedule phase.
Scheduled Implementation End	This field specifies the date and time that the work to implement the change should end. This field becomes required in the Plan and Schedule phase.
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.
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.
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 close the change, the CIs will be set as Up in Configuration Management.
Ex. Project Ref.	This field references an external project number.
Implementation Plan	An assessment of the change, often generated by the Change Implementer, that the Change Coordinator uses to assess the impact of the change to services.
Effect of not Implementing	The impact if not implementing the change. This is a required field.
Change Owner	The name of the user owning the change. This is a required field.
Subcategory	The subcategory is a breakdown of the category and describes the type of change in more detail.
Actual Implementation Start	The time when the implementation actually began.
Actual Implementation End	The time when the implementation actually ended.
Review Results	Results of the review after Post Implementation Review, this is a required field.

Change Management field descriptions, continued

Label	Description
Closure Code	<p>The completion code indicates the way a change is closed.</p> <p>VALID VALUES</p> <ul style="list-style-type: none"> • 1 - Successful • 2 - Successful (with problems) • 3 - Failed • 4 - Rejected • 5 - Withdrawn • 6 - Cancelled
Associated CIs section> Completed/Cancelled CMDB Modifications	<p>The data in this section is used by the UCMDB integration whenever there are past changes to the values registered for the CI.</p>
Affected Services section> Affected Services	<p>This 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.</p>
Approvals section> Current Approvals>	<p>This section provides an overview of the current approvals related to any changes for the CI, and important information such as approval status, and approvers as well. 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.</p> <p>The data displayed includes the following information:</p> <ul style="list-style-type: none"> • Approval Type • Approval Status • # Approved • # Denied • # Pending

Change Management field descriptions, continued

Label	Description
Approvals section> Approval Log>	This subsection 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: <ul style="list-style-type: none"> • Action • Approver/Operator • By • Date/Time • Phase
Reason for Change	A code that indicates the primary reason for implementing the request. Examples of reason codes are Incident/Problem Resolution and Business Requirement.
Approval section> Pending Reviews	The name(s) of the groups or operator IDs that should review the change for the CI after it has been approved.
Tasks	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 in the Tasks section. The data displayed includes the following information: <ul style="list-style-type: none"> • Task No • Phase • Status • 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 all changes while backing out a change. 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.

Chapter 5

Service Desk 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 Service Desk Interaction Management processes.

Topics in this section include:

- ["Service Desk within the ITIL framework" below](#)
- ["Service Desk application" on the next page](#)
- ["Service Desk process overview" on the next page](#)
- ["Input and output for Service Desk Interaction Management" on page 60](#)
- ["Key performance indicators for Service Desk Interaction Management" on page 61](#)
- ["RACI matrix for Service Desk Interaction Management" on page 62](#)

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.

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 knowledge base, 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 if a reported issue requires further action. It can also be added to a record in another Service Manager application, such as Change Management.

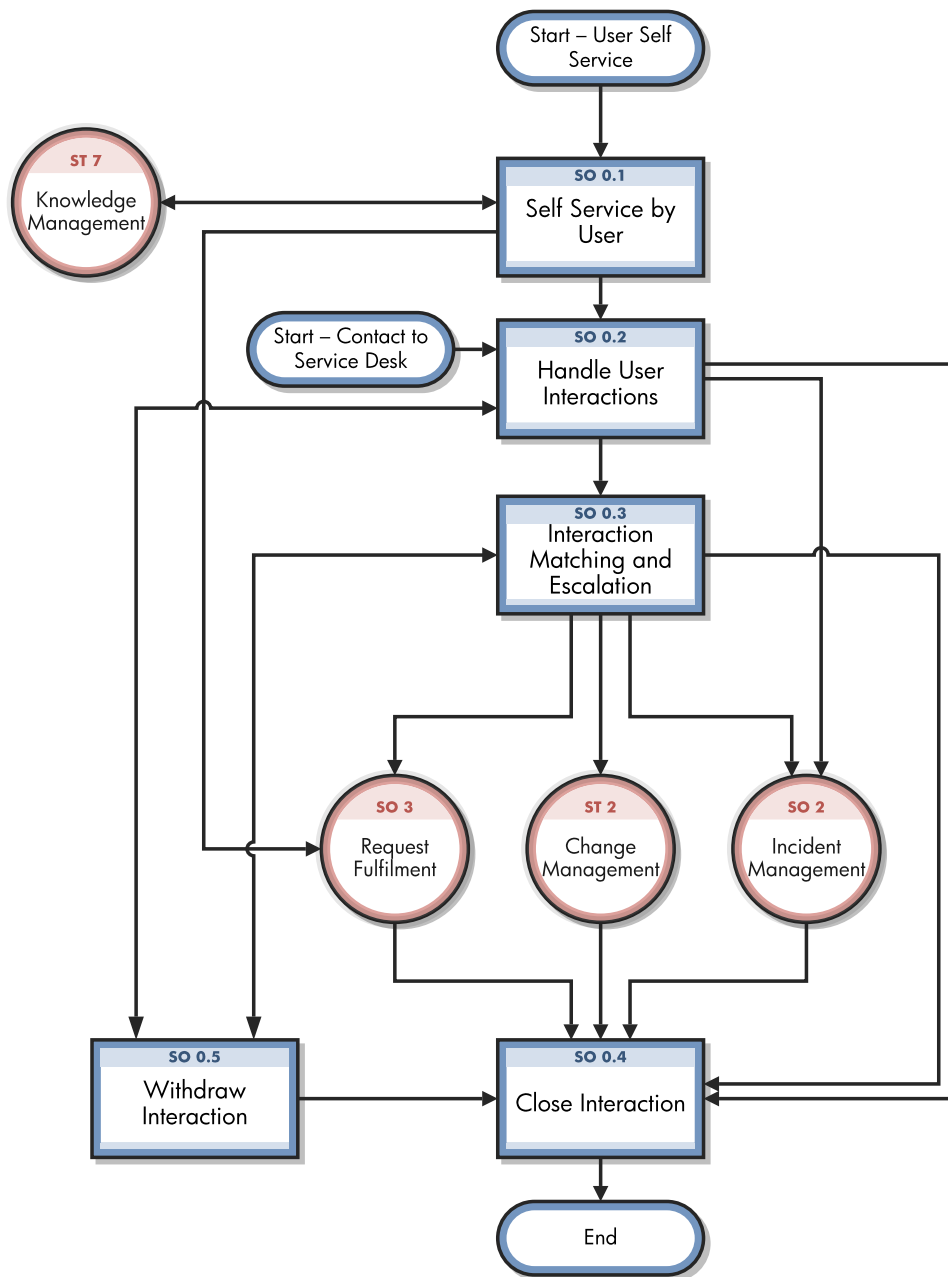
Service Desk process overview

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, E-mail, 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 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 below. They are described in detail in "[Service Desk Workflows](#)".



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, problems, or known errors 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.

- If an existing incident 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.

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

- The user contacts the service desk for assistance.
- The Service Desk agent populates an interaction record with the relevant information.
- Because the issue cannot be resolved immediately, the Service Desk agent opens an incident, and the incident is assigned to a technician.
- The technician discovers that the printer network connection is broken.
- The technician fixes the connection and closes the incident.
- The Service Desk agent contacts the user and instructs the user to attempt printing to the network printer.
- 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 create a new incident and then relate the unsolved interaction.
- 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.

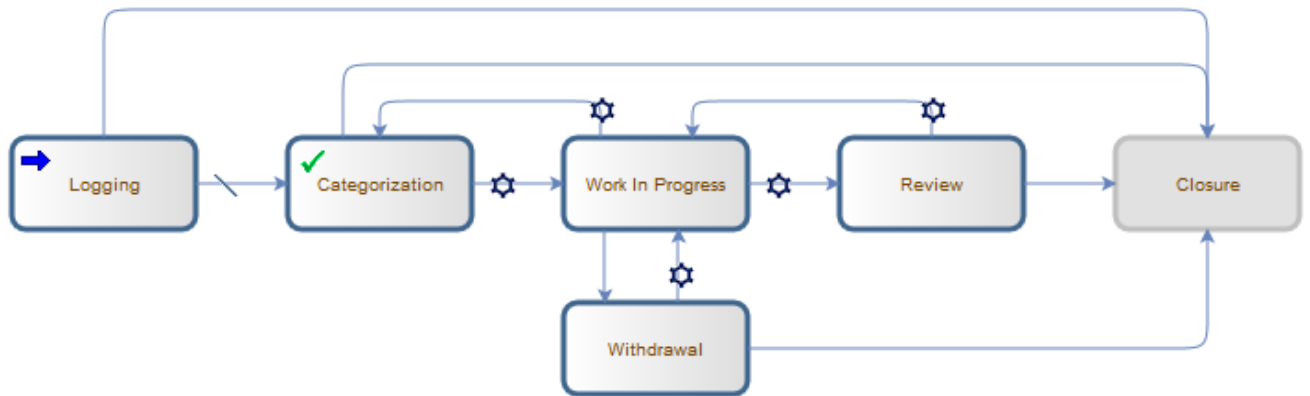
Interaction categories

Service Manager Categories classify and define the type of interaction. Each category could have its own workflow process. The steps of the workflow are represented by the phases. Service Manager requires that every interaction has an interaction category and phases.

Interaction phases

Service Manager uses phases to describe the steps needed to dispose an interaction. The phase also determines the forms users see, the actions users can manually trigger.

The following figure shows the workflow phases for an Interaction.



Service Desk user roles

The following table describes the responsibilities of the User Interaction Management user roles.

User Interaction Management user roles

Role	Responsibilities
User	<ul style="list-style-type: none">• 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.

User Interaction Management user roles, continued

Role	Responsibilities
Service Desk Agent	<ul style="list-style-type: none"> • 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. • Withdraw Interaction on behalf of a user.

Input and output for Service Desk Interaction Management

Interactions can be triggered and resolved in several ways. The following table outlines the inputs and outputs for the User Interaction Management process.

Input and output for Service Desk Interaction Management

Input to Service Desk Interaction Management	Output from Service Desk Interaction Management
<p>A user can contact the service desk and give input by using instant messages, phone, email, self-service web pages, or other means.</p>	<p>Service desk personnel can handle an interaction in the following ways:</p> <ul style="list-style-type: none"> • 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 Service Desk Interaction Management

The Key Performance Indicators (KPIs) in the following table are useful for evaluating your indicators for Service Desk 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.

Key Performance Indicators for Service Desk 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 and going through the whole service desk workflow
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 Service Desk 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 Service Desk Interaction Management is shown in the following table.

RACI matrix for Service Desk 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 Matching and Escalation	R	R	A
SO 0.4	Interaction Closure	R/I	R	A
SO 0.5	Withdraw Interaction	R/I	R	A

Chapter 6

Service Desk 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, problem 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 \(process SO 0.1\)" on the next page](#)
- ["Interaction Handling \(process SO 0.2\)" on page 68](#)
- ["Interaction Matching and Escalation \(process SO 0.3\)" on page 72](#)
- ["Interaction Closure \(process SO 0.4\)" on page 75](#)
- ["Withdraw Interaction \(process SO 0.5\)" on page 79](#)

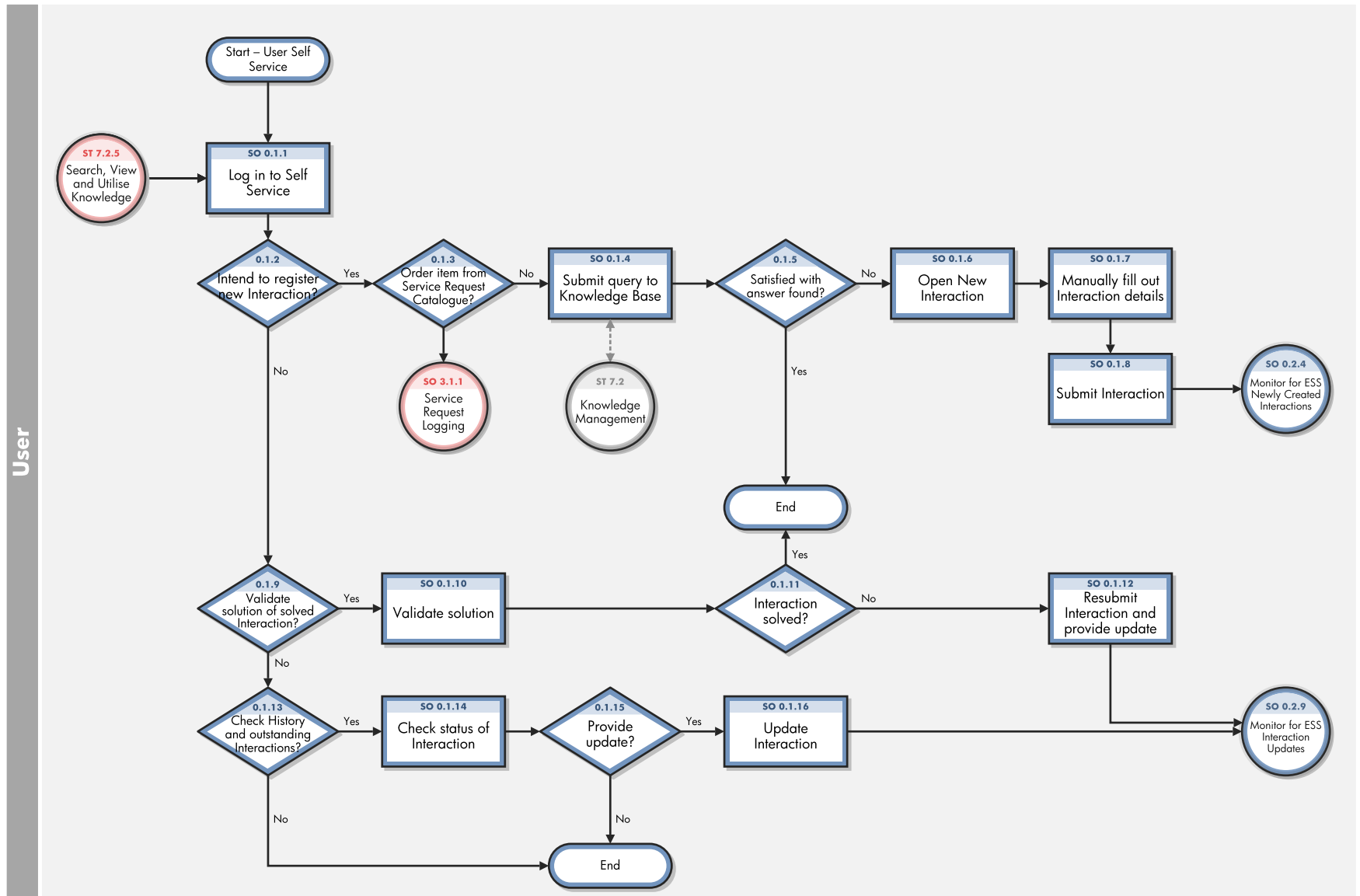
Self-Service by User (process SO 0.1)

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.

Self-Service by User (SO 0.1) is illustrated in the following figure:



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	Intend to 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 Request Catalog?	If yes, log a service request. If no, go to SO 0.1.4.	User
SO 0.1.4	Submit query to Knowledge Base	To search for a knowledge document, users must complete a search.	User
SO 0.1.5	Satisfied with answer found?	If yes, stop. If not, go to SO 0.1.6.	User
SO 0.1.6	Open new interaction	To open a new interaction from the knowledge search screen, users must create a New Interaction.	User
SO 0.1.7	Manually fill out interaction details	To register a new interaction, users must provide a title and a description of the request; select the urgency, and preferred contact method; and can optionally provide affected Service and add an attachment.	User
SO 0.1.8	Submit interaction	When all mandatory fields are completed, submit the form to send the request to the service desk.	User

Self-Service by User (SO 0.1) process, continued

Process ID	Procedure or Decision	Description	Role
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 Closed 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 not, 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 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
SO 0.1.14	Check status of Interaction	Use View Open Requests to get an overview of all open 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

Self-Service by User (SO 0.1) process, continued

Process ID	Procedure or Decision	Description	Role
SO 0.1.16	Update Interaction	<p>There are two scenarios to update an interaction and have a Save button to save the updated information.</p> <ul style="list-style-type: none">• 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 & Exit 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 an Update button when you select an existing interaction. The interaction is also a status of Dispatched or Callback. Once you have added more information to the request or performed the changes, you can click Save & Exit.	User

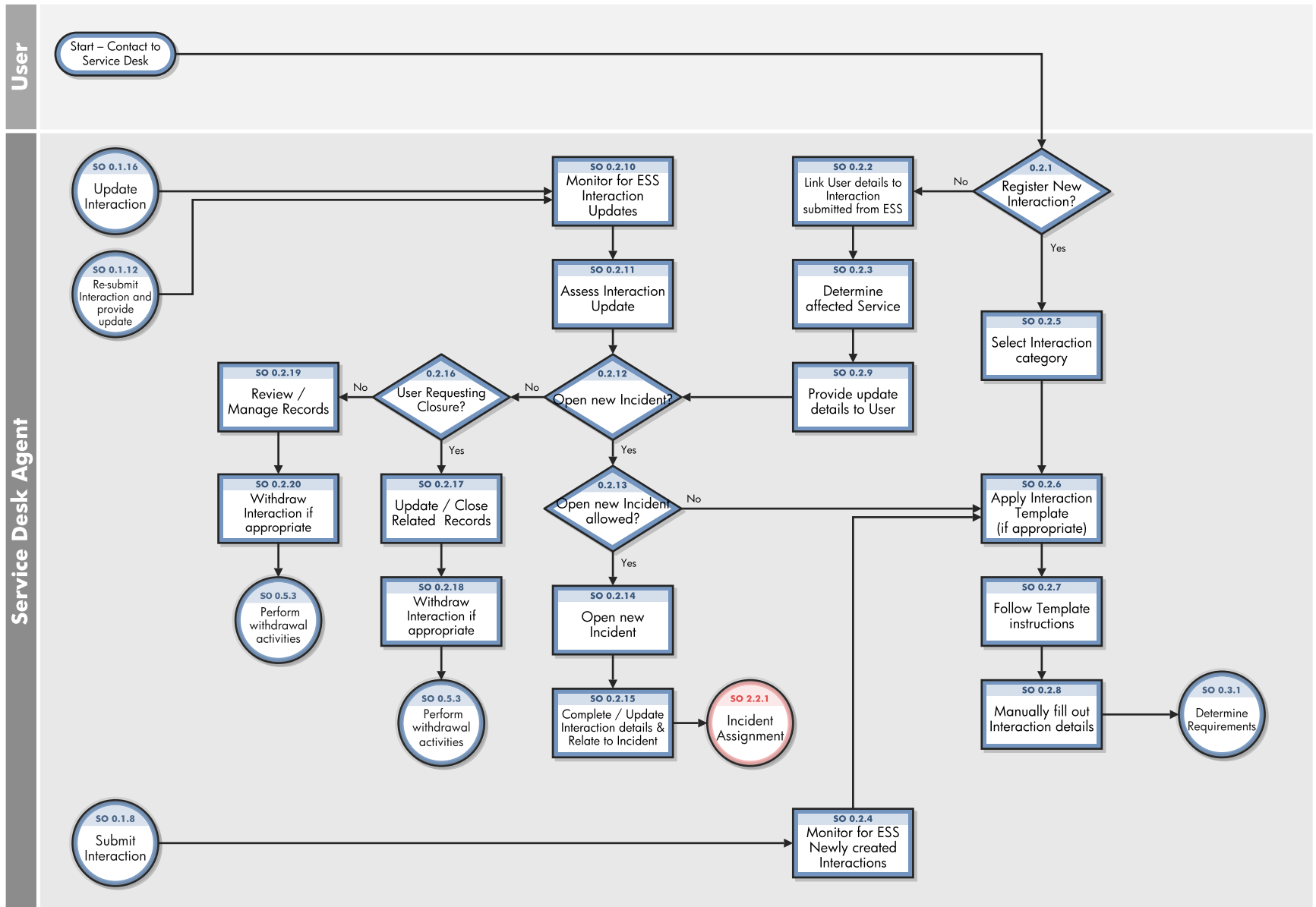
Interaction Handling (process SO 0.2)

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 fulfillment.

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

Interaction Handling (SO 0.2) is illustrated in the following figure:



Interaction Handling (SO 0.2) process

Process ID	Procedure or Decision	Description	Role
SO 0.2.1	Register New Interaction?	If the interaction is new, go to SO 0.2.5. If not, go to SO 0.2.2.	Service Desk Agent
SO 0.2.2	Link User details to Interaction submitted from ESS	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 0.2.3	Determine affected service	In the Affected Service field, select the service that matches the user request. Then, go to SO 0.2.9.	Service Desk Agent
SO 0.2.4	Monitor for ESS newly created Interactions	If there are new Interactions, follow the same Interaction registration process.	Service Desk Agent
SO 0.2.5	Select Interaction category	Select the appropriate Interaction category from the available category list, and then go to SO 0.2.6.	Service Desk Agent
SO 0.2.6	Apply Interaction Template (if 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 0.2.7	Follow Template instructions	The predefined fields are filled in from the model.	Service Desk Agent
SO 0.2.8	Manually fill out Interaction details	Fill out the required interaction details such as short title, a full description, Contact, Service Recipient, and Affected Service. In addition, select the applicable impact and urgency. The assignment group is automatically filled in, based on the Service Desk Group configured in the Service Desk environment record.	Service Desk Agent

Interaction Handling (SO 0.2) process, continued

Process ID	Procedure or Decision	Description	Role
SO 0.2.9	Provide update details to User	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 0.2.10	Monitor for ESS Interaction Updates	If Interactions are updated, they must be reassessed and a new incident may need to be opened.	Service Desk Agent
SO 0.2.11	Assess Interaction Update	Evaluate Interactions that have been updated or resubmitted.	Service Desk Agent
SO 0.2.12	Open new Incident?	If the user is unhappy with a solution provided and a new incident must be opened, go to SO 0.2.13. If not, go to SO 0.2.16.	Service Desk Agent
SO 0.2.13	Open new Incident allowed?	If opening a new incident is allowed due to a user request during the period of two weeks after solution notification, go to SO 0.2.14. If not, go to SO 0.2.6.	Service Desk Agent
SO 0.2.14	Open new Incident	Because the previously registered incident was solved incorrectly, open a new incident and provide an update that states the reason that the incident was created.	Service Desk Agent
SO 0.2.15	Complete/Update Interaction details & Relate to Incident	Relate the interaction to the open incident.	Service Desk Agent
SO 0.2.16	User requesting closure?	If the user is requesting the incident be closed, go to SO 0.2.17. If not, go to SO 0.2.19.	Service Desk Agent

Interaction Handling (SO 0.2) process, continued

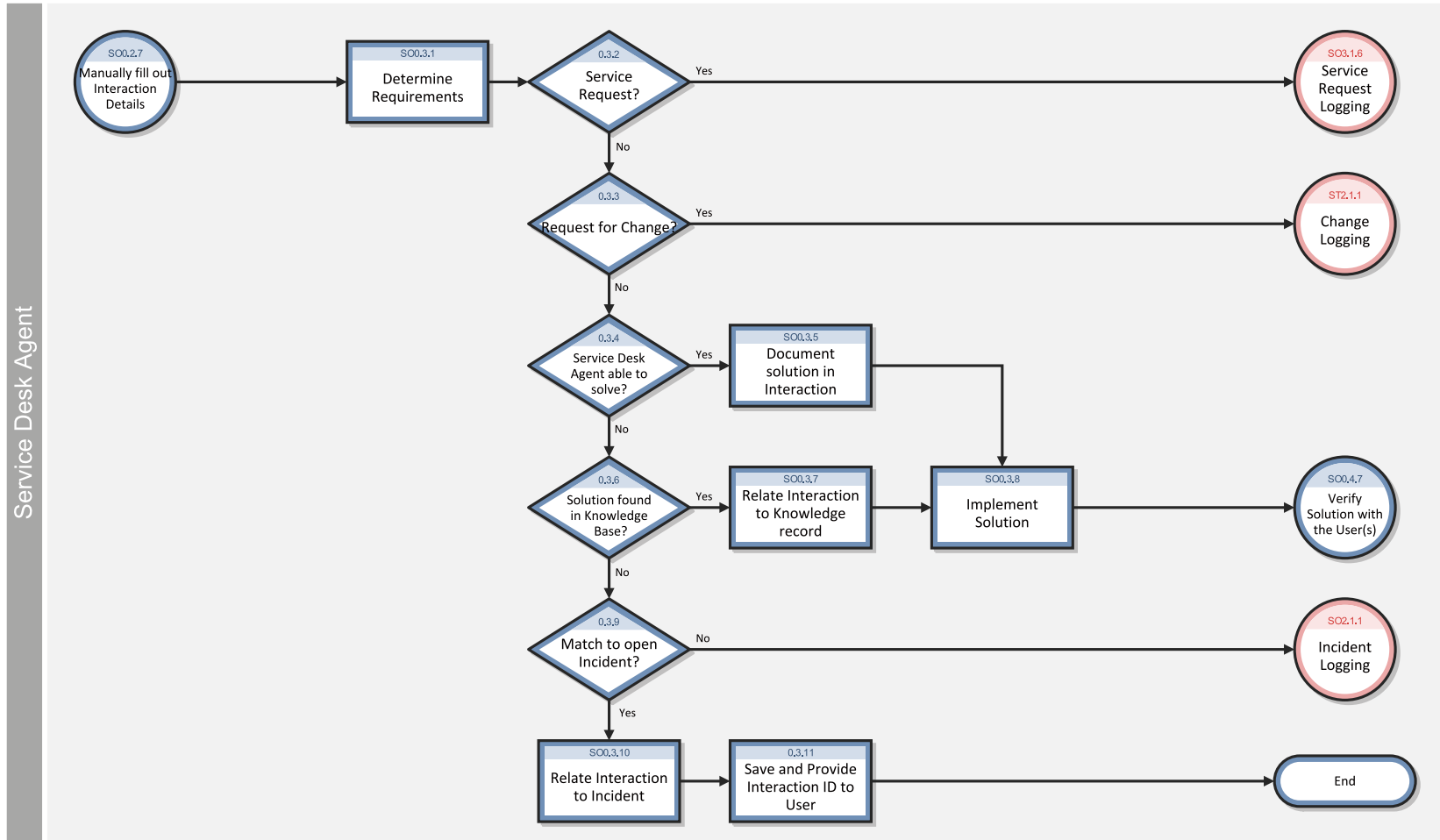
Process ID	Procedure or Decision	Description	Role
SO 0.2.17	Update/Close related records	Update the related record as needed and close it.	Service Desk Agent
SO 0.2.18	Withdraw Interaction if appropriate	Withdraw the interaction if this registration is not needed anymore.	Service Desk Agent
SO 0.2.19	Review/Manage records	Review the records and take action accordingly.	Service Desk Agent
SO 0.2.20	Withdraw Interaction if appropriate	Withdraw the interaction if this registration is not needed anymore.	Service Desk Agent

Interaction Matching and Escalation (process SO 0.3)

When an Interaction is received, the Service Desk Agent first determines if the Interaction is a service request or a request for change, and if so, logs the request. If the Service Desk Agent is not able to resolve the issue, the incident can either be related to an existing incident or logged as a new incident.

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

Interaction Matching and Escalation (SO 0.3) is illustrated in the following figure:



Interaction Matching and Escalation (SO 0.3) process

Process ID	Procedure or Decision	Description	Role
SO 0.3.1	Determine Requirements	After filling out the Interaction details, the Service Desk Agent determines what requirements of the request.	Service Desk Agent
SO 0.3.2	Service Request?	If a service request is needed, the Service Desk agent logs the request. If not, proceed to SO 0.3.3.	Service Desk Agent
SO 0.3.3	Request for Change?	If a change is required, log the change request. If not, proceed to SO 0.3.4.	Service Desk Agent
SO 0.3.4	Service Desk Agent able to solve?	If the Service Desk agent is able to solve the request, proceed to SO 0.3.5. If not, proceed to SO 0.3.6.	Service Desk Agent
SO 0.3.5	Document solution in Interaction	The Service Desk agent documents the solution implemented.	Service Desk Agent
SO 0.3.6	Solution found in Knowledge Base?	If the solution is already documented in the Knowledge Base, proceed to SO 0.3.7. If not, proceed to SO 0.3.9.	Service Desk Agent
SO 0.3.7	Relate Interaction to Knowledge record	The Service Desk Agent selects “use solution” in the knowledge record to record this as the knowledge source and auto populate details of the solution in the Interaction record solution field.	Service Desk Agent
SO 0.3.8	Implement Solution	The Service Desk Agent then implements the solution for the User.	Service Desk Agent

Interaction Matching and Escalation (SO 0.3) process, continued

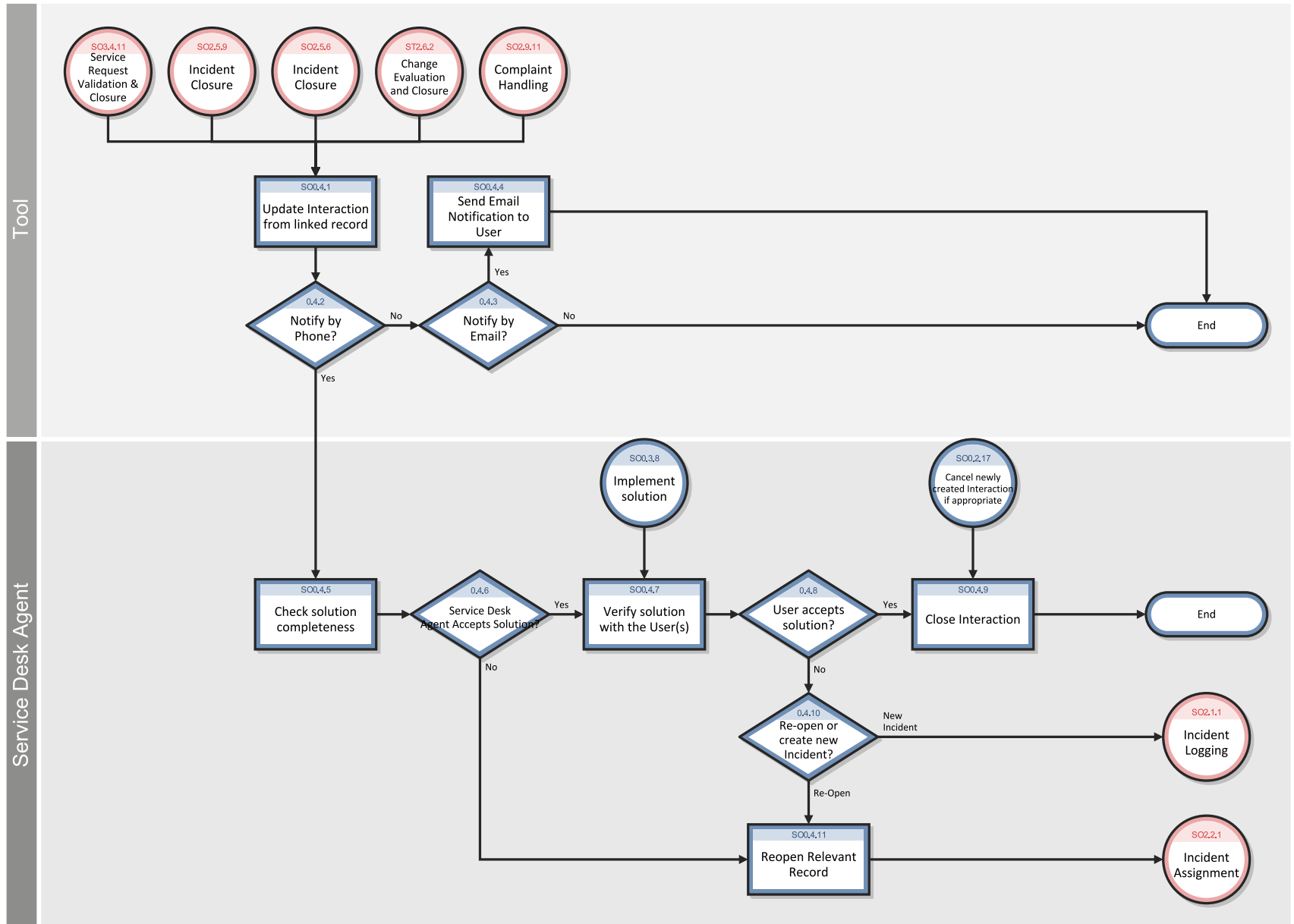
Process ID	Procedure or Decision	Description	Role
SO 0.3.9	Match to open Incident?	The Service Desk Agents checks to see whether another open incident is similar to the new request, and if a match can be made. If a match can be made, proceed to SO 0.3.10. If not, log the incident.	Service Desk Agent
SO 0.3.10	Relate Interaction to Incident	If an open incident matches the new request, the Service Desk Agent relates the two.	Service Desk Agent
SO 0.3.11	Save and Provide Interaction ID to User	The Service Desk Agent saves the incident and provides the Interaction ID to the User.	Service Desk Agent

Interaction Closure (process SO 0.4)

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.

Interaction Closure (SO 0.4) is illustrated in the following figure:



Interaction Closure (SO 0.4) process

Process ID	Procedure or Decision	Description	Role
SO 0.4.1	Update Interaction from linked record	The Interaction could involve the closure of an incident, change request, or service request, or the submission of a complaint.	Service Desk Agent
SO 0.4.2	Notify by phone?	If the Notify By method states that the user wants to be notified by phone, go to SO 0.4.5. If not, go to SO 0.4.3.	Service Desk Agent
SO 0.4.3	Notify by email?	If the Notify By method states that the user wants to be notified by email, go to SO 0.4.4. If not, the User does not need to be notified.	Service Desk Agent
SO 0.4.4	Send email notification to User	Send the email notification.	Service Desk Agent
SO 0.4.5	Check solution completeness	The Service Desk agent checks the solution provided for all Callback interactions.	Service Desk Agent
SO 0.4.6	Service Desk Agent accepts solution?	If yes, go to SO 0.4.7. If not, go to SO 0.4.11.	Service Desk Agent
SO 0.4.7	Verify solution with the User (s)	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 0.4.8	User accepts solution?	If yes, go to SO 0.4.9. If no, go to SO 0.4.10.	Service Desk Agent

Interaction Closure (SO 0.4) process, continued

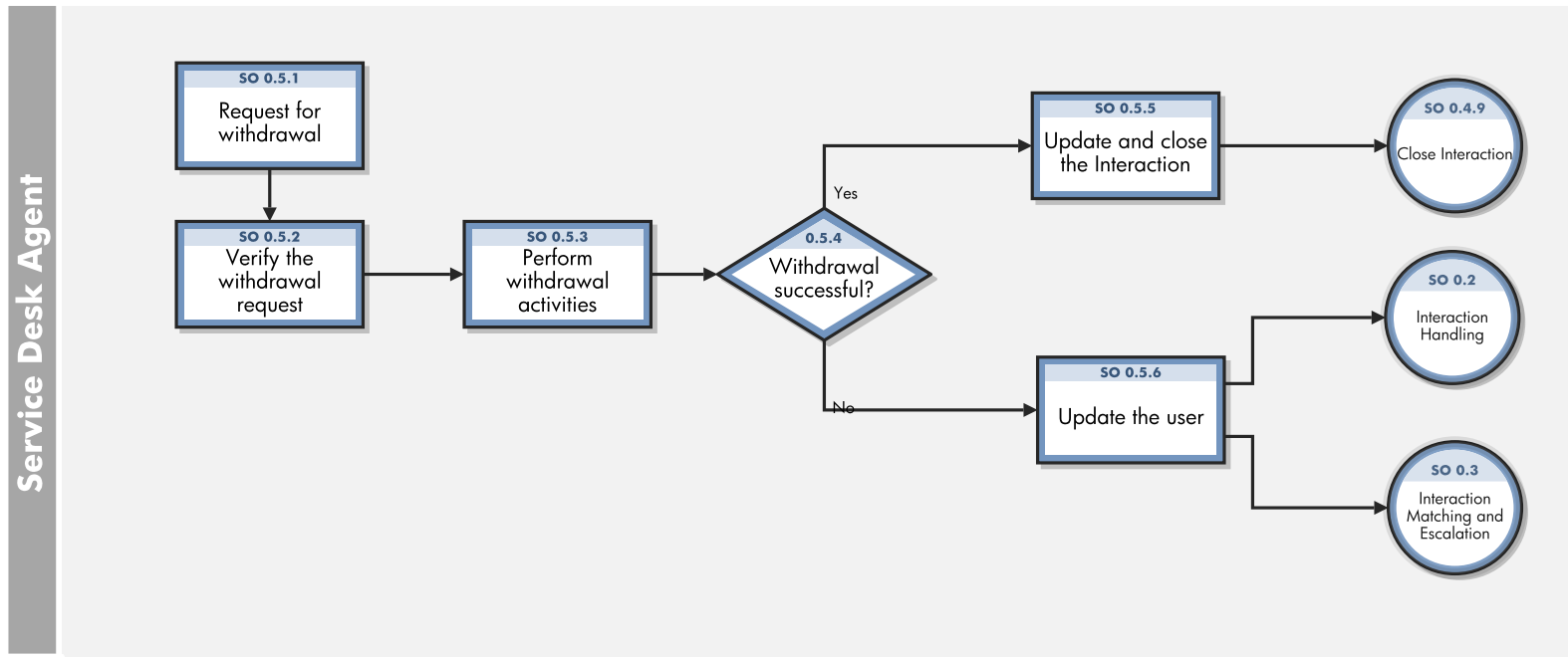
Process ID	Procedure or Decision	Description	Role
SO 0.4.9	Close interaction	The Service Desk Agent closes the interaction.	Service Desk Agent
SO 0.4.10	Reopen or Create new Incident	The solution provided may not solve the issue for all users. If the solution does not solve the issue for all users, the Service Desk Agent must either reopen the existing record or log the incident.	Service Desk Agent
SO 0.4.11	Reopen relevant record	The Service Desk agent reopens the incident for further investigation and diagnosis.	Service Desk Agent

Withdraw Interaction (process SO 0.5)

The Withdraw Interaction process identifies the steps to withdraw an interaction.

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

Withdraw Interaction (process SO 0.5) is illustrated in the following figure:



Withdraw Interaction (SO 0.5) process

Process ID	Procedure or Decision	Description	Role
SO 0.5.1	Request for withdrawal	The user contact the Service Desk Agent and ask for the interaction to be withdrawn on their behalf by providing appropriate information.	Service Desk Agent
SO 0.5.2	Verify the withdrawal request	The Service Desk Agent verifies the request to check whether the Interaction can be withdrawn or not.	Service Desk Agent
SO 0.5.3	Perform withdrawal activities	The Service Desk Agent performs withdrawal activities for the request.	Service Desk Agent
SO 0.5.4	Withdrawal successful?	If the withdrawal is successful, go to SO 0.5.5. If not, go to SO 0.5.6.	Service Desk Agent
SO 0.5.5	Update and close the Interaction	The user is informed about the Interaction withdrawal and go to SO 0.4.9 to close the Interaction.	Service Desk Agent
SO 0.5.6	Update the user	The user is communicated on the reason why the Interaction cannot be withdrawn. The Interaction moves to the previous status and the provisioning continues.	Service Desk Agent

Chapter 7

Service Desk Details

HP Service Manager uses its Service Desk application to enable the Service Desk Interaction Management process. The main function of Service Manager 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" on the next page](#)
- ["Interaction form after escalation" on page 83](#)
- ["Service Desk Interaction Management form details" on page 84](#)
- ["Interaction categories" on page 95](#)

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.

A new interaction that has been filled in is illustrated in the following screenshot:

Interaction - SD10366

Interaction ID:	<input type="text" value="SD10366"/>	<input type="checkbox"/> Reported Via Self Service
Handle Time:	<input type="text" value="00:17:13"/>	
Contact:	<input type="text" value="ADAMS, IRENE"/>   	Phase:
Notify By:	<input type="text" value="E-mail"/> 	Categorization:
Affected Service:	<input type="text" value="MyDevices"/>   	Status:
Affected CI:	<input type="text" value=""/>   	Approval Status:
Title:	<input type="text" value="Desktop reboots with BIOS message"/>	
Description:	<input type="text" value="Desktop reboots with BIOS message CPU temperature"/>	

Category and Assignment

Category:	<input type="text" value="incident"/>	Impact:	<input type="text" value="4 - User"/>
Subcategory:	<input type="text" value="hardware"/> 	Urgency:	<input type="text" value="3 - Average"/>
Area:	<input type="text" value="hardware failure"/> 	Priority:	<input type="text" value="3 - Normal"/>
Assignment Group:	<input type="text" value="Service Desk"/> 	Service Recipient:	<input type="text" value="EMPLOYEE, JOE"/>   
Assignee:	<input type="text" value=""/> 		

Interaction form after escalation

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

The same interaction after escalation is illustrated in the following screenshot:

Related Records - (1)

Link Type:

All Related Records

ID	Type	Phase	Status	Title
IM10141	Escalate To	Categorization	Categorize	Desktop reboots with BIOS message

Activities

New Update Type: Visible to Customer

New Update:

Journal Updates:

Activity Type:

Date/Time	Type	Operator	Description
06/02/13 22:46:52	Priority Change	falcon	Priority changed from NONE to 3
06/02/13 22:46:52	Status Change	falcon	Status changed to "Categorize"
06/02/13 22:46:52	Phase Change	falcon	The Interaction Phase Changed from "Logging" to "Categorization"
06/02/13 22:46:51	Open	falcon	Desktop reboots with BIOS message CPU temperature

Service Desk Interaction Management form details

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

Service Desk 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.

Service Desk Interaction Management form details, continued

Label	Description
Status	<p>The options in this field have been revised to align with our new best practices.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Tip: You may want to tailor these options to match your business needs.</p> </div> <p>These statuses are available out-of-box:</p> <ul style="list-style-type: none"> • Open — The interaction has been initially logged. For example, when the Service Desk Agent is still on the phone with the customer. • Categorize — The interaction has been logged and saved by Service Desk Agent, or a request has been created by a self-service user. The categorization details will be provided with this status. • Assign — The status is manually set by Service Desk Agent, or a service catalog request will stay in this status when it is created by self-service user or Service Desk Agent. The assignment will be made with this status. • Suspended — The interaction can be suspended for a predefined duration at categorization or fulfillment. It will be worked upon only after it is unsuspended either manually or automatically. • In Progress — The interaction has no incidents, changes, or other records related to it. It is fulfilled by Service Desk. • Dispatched — The interaction has been escalated or the catalog request approved and the interaction is now related to another record, such as an incident, change, or request. • Resolved — The interaction has been resolved with solution filled. • Callback — There is an action pending for the interaction. The Service Desk Agent must now call the contact. If the Notify By field for that user is set to Telephone, the interaction is automatically set to Callback when the related record is closed. • Closed — The interaction was closed by the help desk or automatically after the related record was closed. • Withdrawal Requested — The user contacts the Service Desk Agent and ask for the interaction to be withdrawn on their behalf by providing appropriate information.

Service Desk Interaction Management form details, continued

Label	Description
Phase	<ul style="list-style-type: none"> • Logging - The interaction has been initially logged. For example, when the Service Desk Agent is still on the phone with the customer. • Categorization – The interaction is categorized and prioritized in this phase. Assignment is also made in this phase. • Work In Progress – The interaction is under investigation, either by Service Desk or by other process, such as incident, change, or request. • Review – The proposed solution of the interaction is reviewed in this phase. • Closure – The interaction was closed by the help desk or automatically after the related record was closed. • Withdrawal – The interaction is in this phase where the user contacts the Service Desk Agent and ask for the interaction to be withdrawn on their behalf by providing appropriate information.
Contact	<p>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.</p> <p>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 field includes a hover-over form that displays full name, telephone, and email address if available for the contact.</p> <p>This is a required field.</p>
Service Recipient	<p>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.</p> <p>The Service Desk Agent populates this field with the person this issue is registered for. This field includes a hover-over form that displays full name, telephone, and email address if available for the service recipient.</p> <p>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 the service recipient.</p> <p>This is a required field.</p>
Location	<p>The location for which the interaction has been reported. The field is for informational purposes only.</p> <p>Location data is customer and implementation specific.</p>

Service Desk Interaction Management form details, continued

Label	Description
Notify By	<p>To notify the customer when the issue has been resolved, Service Manager prepopulates this field with Email for user. User or the Service Desk Agent can change it to None or Telephone, if applicable.</p> <p>When the related incident or change is closed:</p> <ul style="list-style-type: none">• 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 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 open a new incident. <p>This is a required field.</p>

Service Desk Interaction Management form details, continued

Label	Description
Affected Service	<p>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.</p> <p>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.</p> <p>These business services are available out-of-box:</p> <ul style="list-style-type: none">• 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 <p>Selecting the service:</p> <ul style="list-style-type: none">• May limit the list of affected CIs.• Validates that it is a valid service. <p>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.</p> <p>This is a required field.</p> <p>Tip: You can use the Smart Indicator, positioned at the end of the field, to search for related incidents or problems.</p>

Service Desk Interaction Management form details, continued

Label	Description
Affected CI	<p>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.</p> <p>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 Applications service, you are presented with a list of CIs in the service, as well as those that you own. This field includes a hover-over form that displays Critical CI and Pending Change check boxes to indicate whether or not these attributes apply to the CI.</p> <p>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.</p>
Title	<p>The Service Desk Agent populates this field with a brief description that identifies the interaction.</p> <p>Note: Service Manager searches this field when you do an advanced or expert text search.</p> <p>This is a required field.</p>
Description	<p>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.</p> <p>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.</p> <p>Note: Service Manager searches this field when you do an advanced or expert text search.</p> <p>This is a required field.</p>

Service Desk Interaction Management form details, continued

Label	Description
Completion Code	<p>This field contains a predefined completion 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.</p> <p>Note: You may want to tailor these options to match your business needs.</p> <p>These completion codes are available out-of-box:</p> <ul style="list-style-type: none"> • Automatically Closed • Cancelled • Fulfilled • Invalid • 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
Knowledge Source	<p>This field contains the reference number of the document from the knowledge base document used to solve the issue.</p> <p>If you find a knowledge article by using Search Knowledge, and then click Use Solution in that article to provide the solution to your customer, this field is populated with the Document ID of the document you used.</p> <p>If you do not use a knowledge document or if you do not click Use Solution in the knowledge document, this field is left blank.</p>
Solution	<p>This field contains a description of the solution used for this interaction.</p> <p>Note: Service Manager searches this field when you do an advanced or expert text search.</p>

Service Desk Interaction Management form details, continued

Label	Description
Category	<p>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.</p> <p>The categories are based on ITIL service-centric processes, and therefore focus on enabling assignment, reporting, and operational analysis for knowledge management purposes.</p> <p>From the category list:</p> <ul style="list-style-type: none"> • Complaint/Incident/Request for Information/Request for Administration > Escalate — You can relate the interaction to an existing incident, an existing known error, an existing problem, or create a new incident. • Request for Change > Escalate — Service Manager creates a new change request. • More or More Actions icon > 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. <p>For more information on categories and the subcategories and areas associated with them, see "Interaction categories" on page 95.</p> <p>This is a required field.</p>
Subcategory	<p>The Service Desk Agent populates this field with the subcategory of concern.</p> <p>Service Manager displays different lists of subcategories, depending on the category you selected. For more information on categories and the subcategories and areas associated with them, see "Interaction categories" on page 95.</p> <p>This is a required field.</p>
Area	<p>The third level of classifying an interaction, mainly used for reporting purposes.</p> <p>Service Manager displays different lists of areas, depending on the subcategory you selected. For more information on categories and the subcategories and areas associated with them, see "Interaction categories" on page 95.</p> <p>This is a required field.</p>

Service Desk Interaction Management form details, continued

Label	Description
Assignment Group	<p>The group assigned to work on the interaction. For a description of this field see the Assignment Group field description in the Incident Management form details section in the Service Manager Processes and Best Practices Guide as this field functions similarly. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups.</p> <p>You may want to change the sample assignment groups to meet your own needs. These assignment groups are available out-of-box:</p> <ul style="list-style-type: none"> • Application • Email / Webmail • Field Support • Hardware • Incident Managers • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • Problem Coordinators • Problem Managers • SAP Support • Service Desk • Service Desk Analysts • Service Manager
Assignee	<p>The name of the person assigned to work on this interaction. 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.</p>

Service Desk Interaction Management form details, continued

Label	Description
Impact	<p>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.</p> <p>The stored value can be 1-4, as follows.</p> <ul style="list-style-type: none">• 1 - Enterprise• 2 - Site/Dept• 3 - Multiple Users• 4 - User <p>This is a required field.</p>
Urgency	<p>The urgency indicates how pressing the issue is for the service recipient. The urgency and the impact are used to calculate the priority.</p> <p>The stored value can be 1-4, as follows.</p> <ul style="list-style-type: none">• 1 - Critical• 2 - High• 3 - Average• 4 - Low <p>This is a required field.</p>
Priority	<p>This field describes the order in which to address this interaction in comparison to others. It contains a priority value calculated by $(\text{impact} + \text{urgency})/2$. Decimals are truncated.</p> <p>The stored value based on that calculation can be 1-4, as follows:</p> <ul style="list-style-type: none">• 1 - Critical• 2 - High• 3 - Average• 4 - Low

Service Desk Interaction Management form details, continued

Label	Description
Approval Status	<p>This field is only used when you request something from the catalog.</p> <p>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.</p> <p>These approval statuses are available out-of-box:</p> <ul style="list-style-type: none"> • 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.
Activities	<p>The Activities section records information that the Service Desk Agent enters during the lifecycle of the Interaction. Every time you update an interaction, you can fill in an update on the Activities section (New Update). A log of all the updates is stored on the Journal Updates and activities list. Activities from related records that are flagged as customer visible also display here.</p>
Related Records	<p>The Related Records section contains a list of all related records for the interaction. These may include related incidents, known errors, problems, changes, and quotes.</p>
SLA	<p>The SLA (Service Level Agreement) section displays SLAs related to the interaction.</p> <p>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 in this section may not display immediately.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>

Service Desk Interaction Management form details, continued

Label	Description
Escalate button	<p>The Service Desk Agent clicks this button to create an incident or change from this interaction. The customer's issue could not be solved immediately.</p> <p>When research time is required, the Interaction 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.</p> <p>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.</p> <p>Clicking Escalate starts the Escalate Interaction solution matching.</p> <p>For more information on the Escalate Interaction solution matching, see "Escalate Interaction solution matching" on page 97.</p>
Withdraw button	The Service Desk Agent clicks this button to withdraw the interaction on behalf of the user.
Close Interaction button	The Service Desk Agent clicks this button to close the interaction. The customer's issue was resolved and requires no further action.
Close Invalid Request button	If the interaction is invalid, click this button to close it as an invalid interaction in the Categorization phase.

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 Interaction. The three-level hierarchy (category, subcategory, and 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 subcategory and area, it also is used for to report results and to determine the knowledgebase assignment for the event.

Note: Since the category values represent best practices, customizing this data is not expected. The subcategory and area 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 subcategories and areas, be sure to set them up in a natural easy-to-follow hierarchy.

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

Categories, subcategories, and areas

Category	Subcategory	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	facilities	hardware failure
incident	facilities	miscellaneous
incident	facilities	supplies
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
incident	security	security event/message
incident	security	virus alert
request for administration	grant access	grant access

Categories, subcategories, and areas, continued

Category	Subcategory	Area
request for administration	other	other
request for administration	password reset	password reset
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 solution matching

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

- Escalate Interaction - Incident

You can escalate Interactions in the following categories to Incident:

- compliant
- incident
- request for information
- request for administration

When you escalate an interaction, you can use queries to search for known errors, incidents, or problems matching the title, CI or service value of the interaction. If you find matching records, you can link the records to the interaction.

- Escalate Interaction - RFC

You can escalate Interactions in the following category to RFC:

- request for change

If change is open on Category in settings, when escalate an interaction to RFC, change category list is displayed to be selected for new change request.

If change is open on Change Model in settings, when escalate an interaction to RFC, Change Model list is displayed to be selected for new change request.

Chapter 8

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" below](#)
- ["Incident Management application" on the next page](#)
- ["Incident Management process overview" on page 100](#)
- ["Input and output for Incident Management" on page 105](#)
- ["Key performance indicators for Incident Management" on page 105](#)
- ["RACI matrix for Incident Management" on page 108](#)

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 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 information

The incident includes the information essential to assigning and addressing the incident. Basically, 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.

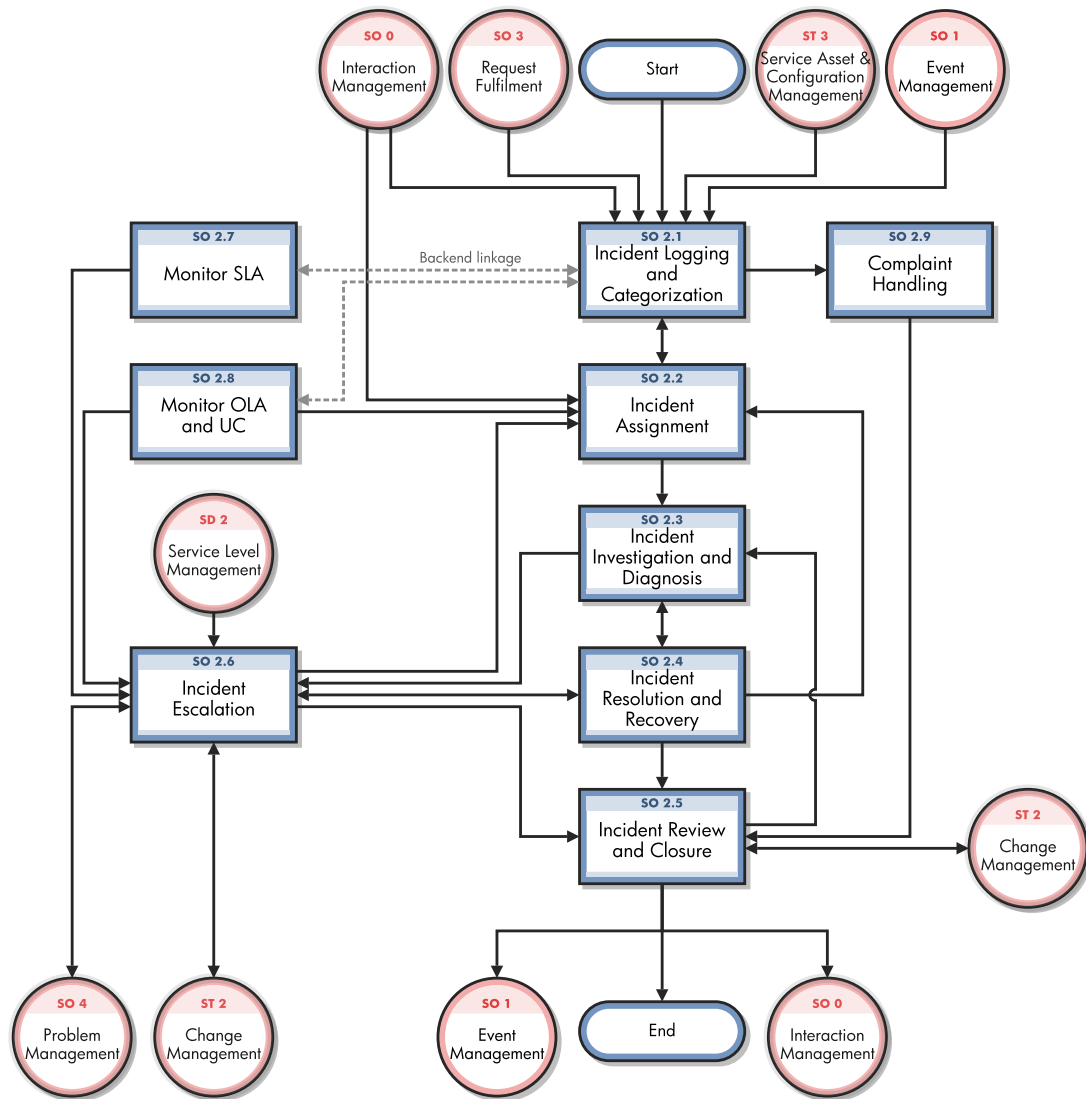
Although the incident does not directly display the information about the person who initiated the incident, that information can be easily retrieved by related interactions in the **Related Records** section.

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

A general overview of the Incident Management processes and workflows is depicted in the figure below. They are described in detail in "[Incident Management Workflows](#)".



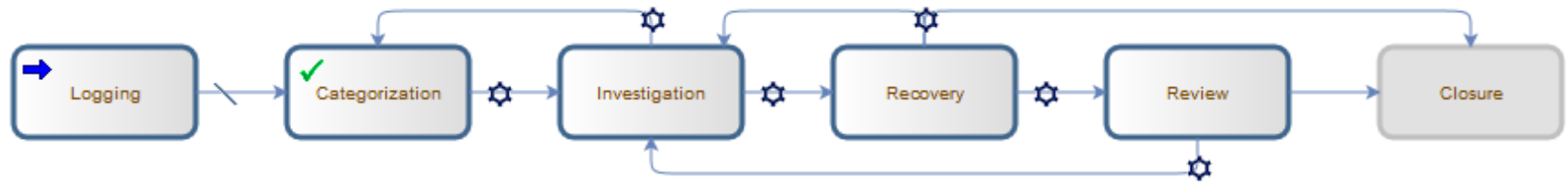
Incident Management categories

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

Incident Management phases

Service Manager uses phases to describe the steps needed to resolve an incident. The phase also determines the forms users see, the actions users can manually trigger.

The following figure shows the workflow phases for an Incident.



Incident Management tasks

Service Manager supports incident tasks to resolve an incident. Incident cannot be closed if there are open Incident tasks underneath it. Except Incident Logging and Closure, each phase can optionally have one or multiple tasks, or no tasks. Each task includes a description, and information about urgency, priority, and assignment.

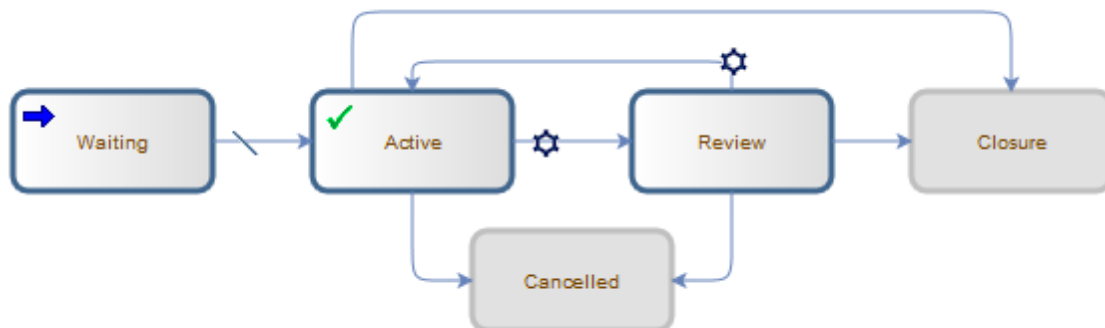
Incident Management tasks include:

- Opening, assigning a task from an incident.
- Searching for a task.
- Managing task categories, status and phases.
- Using the task queue.

Incident Task phases

This section describes the flow of an incident task as it progresses from the 'Waiting' phase to the 'Closed' phase in the Generic Task workflow.

The following figure shows the Incident Task workflow in Process Designer.



Incident Management user roles

The following table describes the responsibilities of the Incident Management user roles.

Incident Management User Roles and Responsibilities

Role	Responsibilities
Operator	Registers incidents based on an event and assigns them to the correct support group.

Incident Management User Roles and Responsibilities , continued

Role	Responsibilities
Service Desk Agent	<ul style="list-style-type: none"> • 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.
Incident Analyst	<ul style="list-style-type: none"> • Reviews assigned incidents. • Investigates and diagnoses incidents. • Create incident tasks to investigate and diagnose incidents. • Documents incident resolutions or workarounds in the Service Management application. • Implements incident resolutions. • Verifies that incidents are resolved and closes them. • Create Incident tasks to implement incident resolutions.
Incident Coordinator	<ul style="list-style-type: none"> • Reviews 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 Management User Roles and Responsibilities , continued

Role	Responsibilities
Incident Manager	<ul style="list-style-type: none"> 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.

Input and output for Incident Management

Incidents can be triggered and resolved in several ways. The following table outlines the inputs and outputs for the Incident Management process.

Input and output for Incident Management

Input to Incident Management	Output from Incident Management
<ul style="list-style-type: none"> Customer interactions with the Service Desk, which can be escalated to incidents Event management tool, which automatically opens incidents Support staff¹ 	<ul style="list-style-type: none"> Resolved incidents Documented workarounds, solutions, or knowledge articles New problems, changes, or incidents <p>Incidents can also trigger several other Service Manager processes, as described in the next section.</p>

¹Service 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 the following table 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.

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.

Key Performance Indicators for Incident Management, continued

Title	Description
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 the following table.

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 and Categorization	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 Review and 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

Chapter 9

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 and Categorization \(process SO 2.1\)" on the next page](#)
- ["Incident Assignment \(process SO 2.2\)" on page 113](#)
- ["Incident Investigation and Diagnosis \(process SO 2.3\)" on page 117](#)
- ["Incident Resolution and Recovery \(process SO 2.4\)" on page 121](#)
- ["Incident Review and Closure \(process SO 2.5\)" on page 124](#)
- ["Incident Escalation \(process SO 2.6\)" on page 126](#)
- ["SLA Monitoring \(process SO 2.7\)" on page 131](#)
- ["OLA and UC Monitoring \(process SO 2.8\)" on page 134](#)
- ["Complaint Handling \(process SO 2.9\)" on page 137](#)

Incident Logging and Categorization (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 incidents, future assigned support group personnel are better able to resolve recorded incidents.

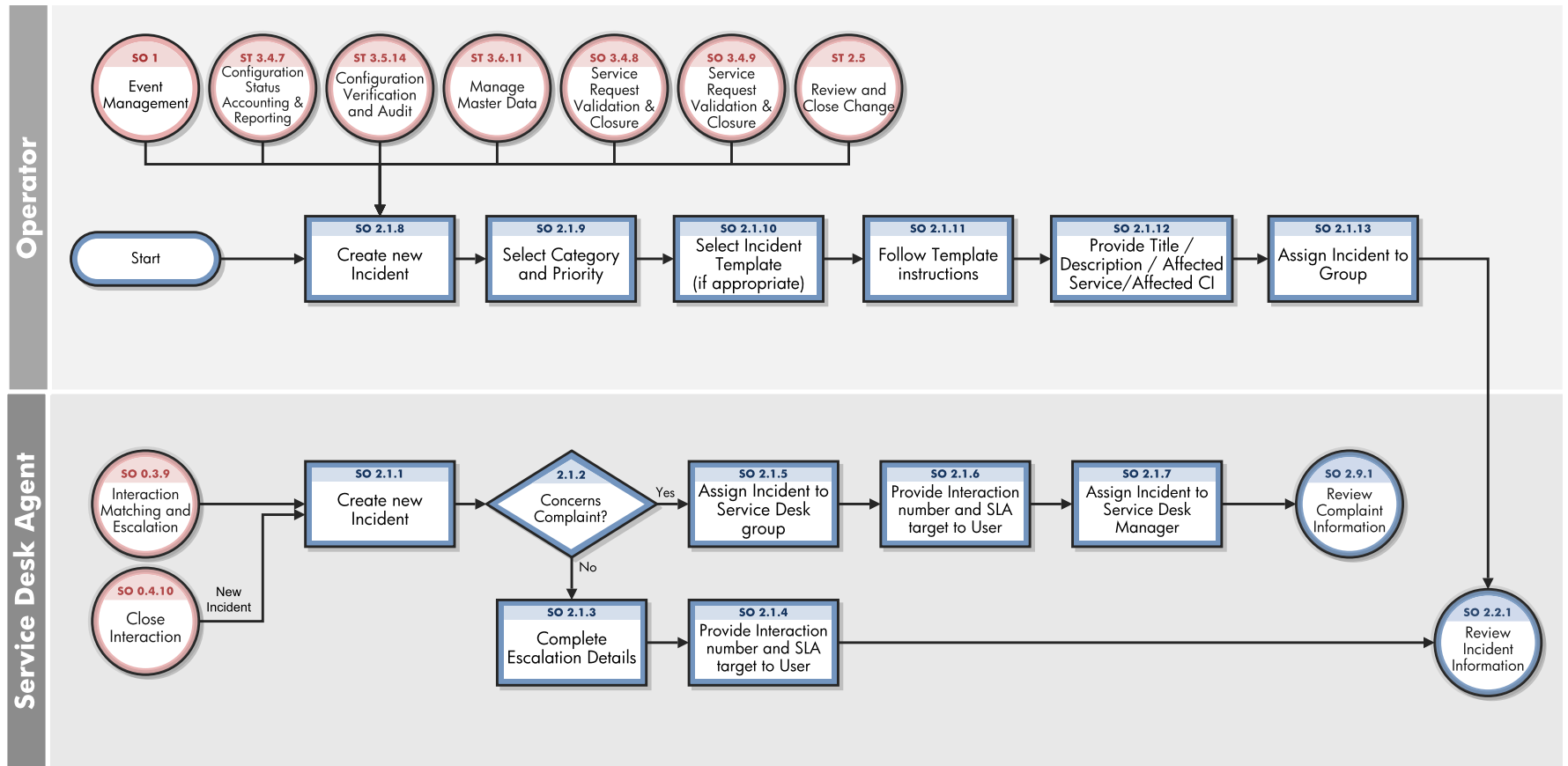
- If the incident is logged by the Service Desk Agent, most incident details are already provided by the interaction record. The Service Desk Agent verifies the Assignment Group to make sure the selected group is the most suitable group to solve the incident. If an incident is categorized as a complaint, 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.

Incident Logging and Categorization workflow is illustrated in the following figure:



Incident Logging and Categorization 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 Service Manager 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	Concerns complaint?	Does the incident concern 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	Complete Escalation Details	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 incident to Service Desk group	Incidents categorized as complaints should be 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 2.9.1).	Service Desk Agent
SO 2.1.8	Create new Incident	An Incident is detected when monitoring the IT infrastructure. The Operator (or Initiator) decides to create an Incident manually or an Incident is generated automatically, depending on tool settings. Go to SO 2.1.10 to select an Incident template (if appropriate).	Operator

Incident Logging and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.1.9	Select Category and Priority	Select the suitable Category and Priority by selecting the applicable impact level and urgency.	Operator
SO 2.1.10	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 2.1.11	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
SO 2.1.12	Provide Title/Description/Affected Service/Affected CI	Provide a suitable title and description for the incident. This might be based on the event text. If possible, the affected Service, affected Configuration Item should be selected.	Operator
SO 2.1.13	Assign incident to group	The incident is manually assigned to the responsible support group, based on the incident categorization and the associated affected services.	Operator

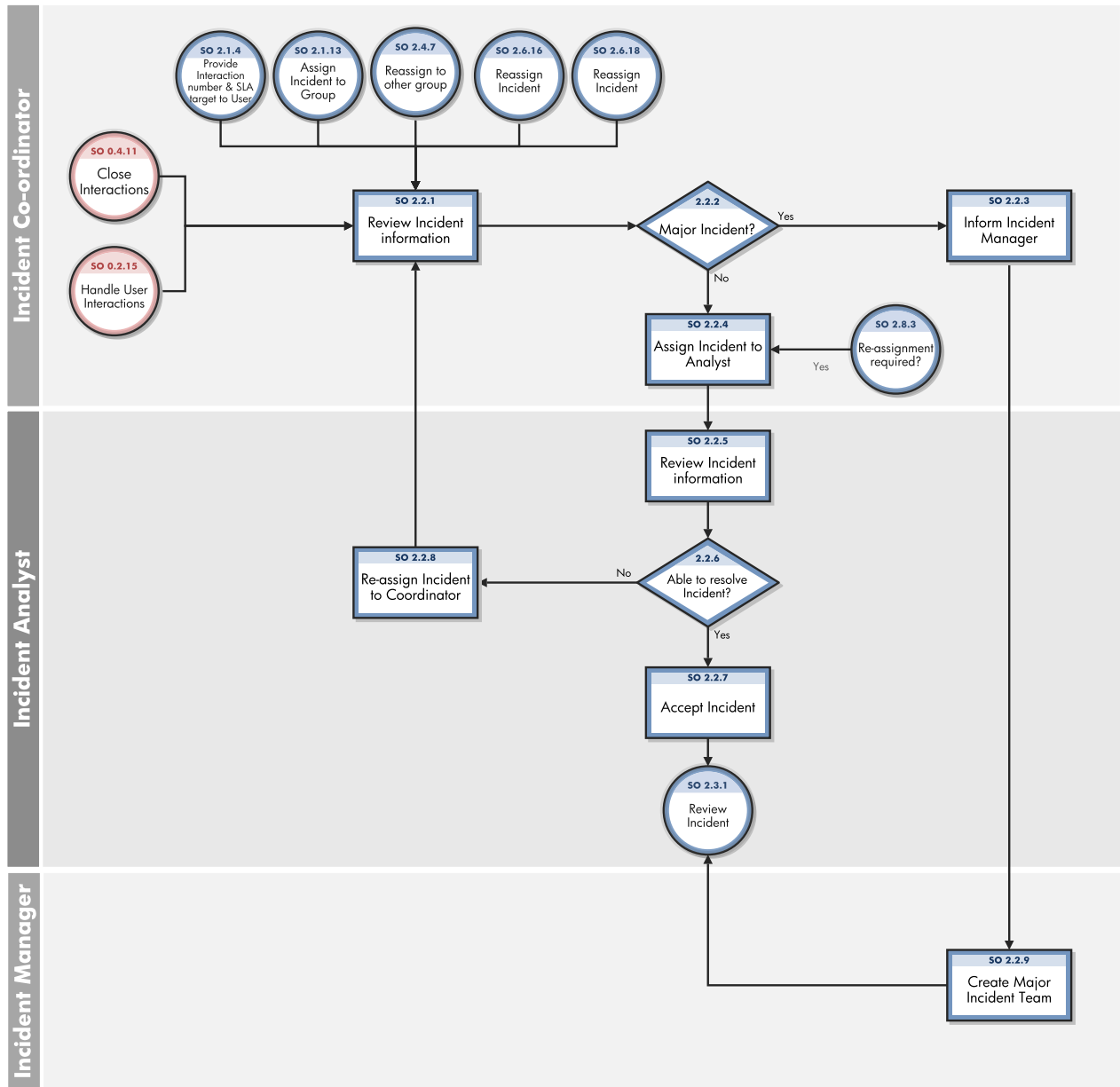
Incident Assignment (process SO 2.2)

Incidents are logged from an interaction by a Service Desk Agent or from an event by an Operator. The Incident Coordinator monitors the incident queue and reviews open status incidents. The Incident Coordinator verifies whether an incident is a major incident using predefined criteria. If it is, the Incident Manager is informed about the incident arrival; otherwise, 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 reassigns it to the Incident Coordinator.

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

Incident Assignment workflow is illustrated in the following figure:



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	Major Incident?	The Incident Coordinator verifies whether this incident is a major incident using predefined criteria. If yes, continue with SO 2.2.3. If no, go to SO 2.2.4	Incident Coordinator
SO 2.2.3	Inform Incident Manager	The Incident Coordinator informs the Incident Manager about the major incident. The Major Incident check box is checked and the ticket is assigned to the manager. Automatic notifications about the Major Incident arrival are sent to Incident Manager. Then go to SO 2.2.9.	Incident Coordinator
SO 2.2.4	Assign Incident to analyst	The Incident Coordinator assigns it to an Incident Analyst from the Incident Coordinator's group for further investigation and diagnosis.	Incident Coordinator
SO 2.2.5	Review Incident information	The Incident Analyst monitors the queue of incidents assigned to him/her and reviews the incoming incidents.	Incident Analyst
SO 2.2.6	Able to resolve Incident?	The Incident Analyst reviews the assigned incident to see if he/she can resolve it. If yes, continue with SO 2.2.7. If no, go to SO 2.2.8.	Incident Analyst
SO 2.2.7	Accept Incident	The Incident Analyst accepts the incident.	Incident Analyst

Incident Assignment process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.2.8	Reassign Incident to coordinator	<p>The Incident Analyst reassigns the incident to the Incident Coordinator if no resolution can be found. The analyst also provides the information on the current status, work performed on the incident, and information on reassignment.</p> <p>The Incident Coordinator can decide whether to escalate the incident, reassign the incident, or close the incident.</p>	Incident Analyst
SO 2.2.9	Create Major Incident Team	<p>The Incident Manager dynamically establishes a separate major incident team under the Incident Manager's direct leadership. The team is tasked to concentrate on this incident exclusively to ensure that adequate resources and focus are provided to find a swift resolution. The Incident Manager forms separate technical teams. Throughout, the Incident Coordinator and Service desk ensures that all activities are recorded and Users are kept updated and fully informed of the progress. A separate procedure with shorter timescales and greater urgency must be used for major incidents.</p>	Incident Manager

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, 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)

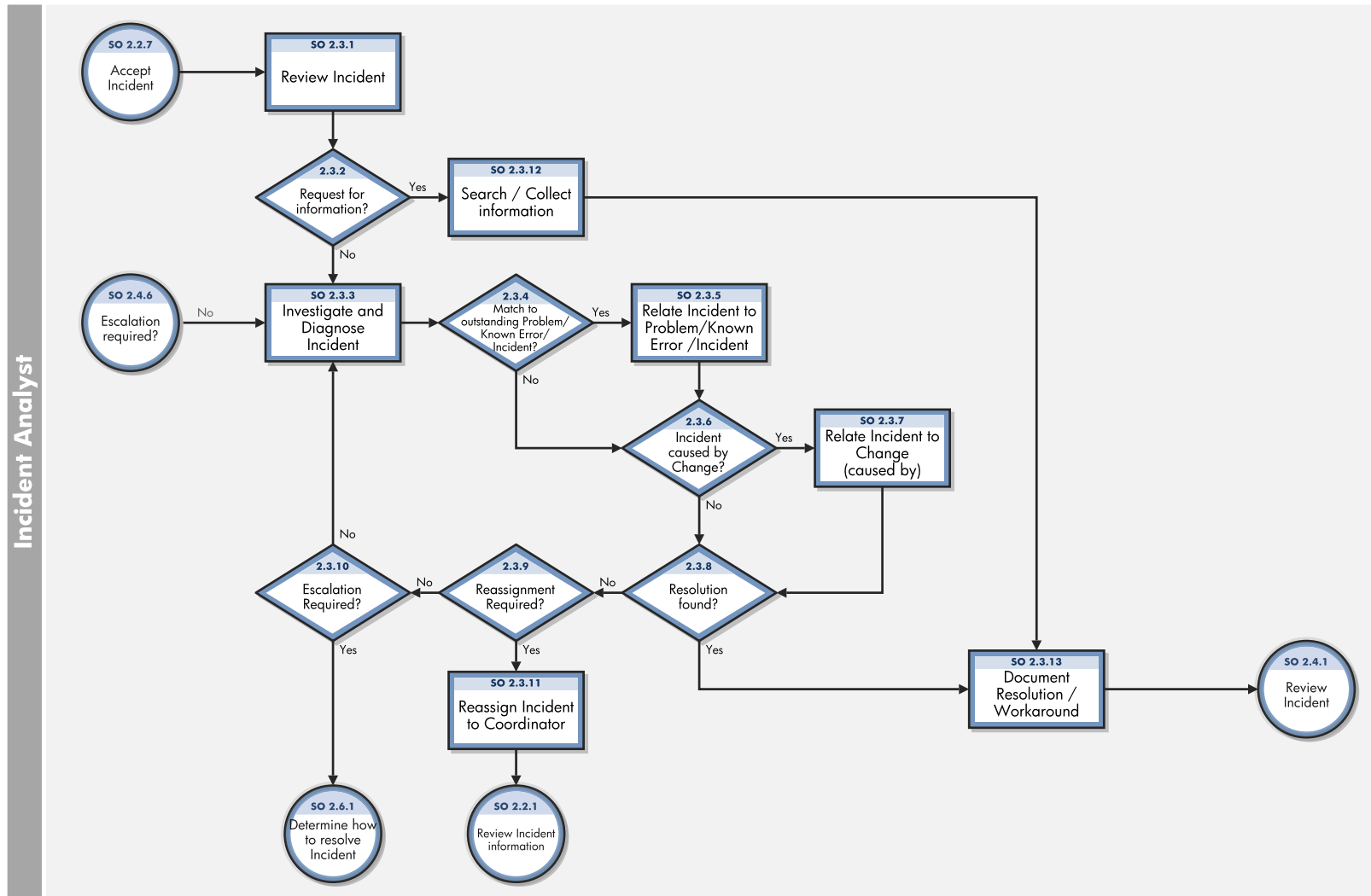
- Searching known errors or the knowledgebase for a workaround or resolution
- Discovering any previous occurrences, including previously logged incident or problems and known errors, the knowledgebase, and error logs and knowledgebases of associated manufacturers and suppliers
- Identifying and registering 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.

Incident Investigation and Diagnosis workflow is illustrated in the following figure:



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 2.3.12. If no, go to SO 2.3.3.	Incident Analyst
SO 2.3.3	Investigate and Diagnose Incident	The Incident Analyst starts to investigate and diagnose the cause of the incident. The status of the incident is set to Work in Progress. Tasks could be created for carrying out the investigation activities.	Incident Analyst
SO 2.3.4	Match to outstanding Problem/ Known Error/ Incident?	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 2.3.5. If no, go to SO 2.3.6.	Incident Analyst
SO 2.3.5	Relate incident to Problem/ Known Error/ Incident	When an incident matches an outstanding problem or known error, the incident is related to the problem or known error record.	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 2.3.7. If no, go to SO 2.3.8.	Incident Analyst
SO 2.3.7	Relate incident to change (caused by)	When the incident is caused by a previous change, the incident is related to the change request. A solution still needs to be found to solve the incident.	Incident Analyst
SO 2.3.8	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 2.3.13. If no, go to SO 2.3.9.	Incident Analyst

Incident Investigation and Diagnosis process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.3.9	Reassignment Required?	If reassignment is required, go to SO 2.3.11. Otherwise, go to SO 2.3.10.	Incident Analyst
SO 2.3.10	Escalation Required	If a solution has not been identified review whether to escalate the Incident to the Incident Coordinator. If yes, go to SO 2.6.1 to determine how to resolve the Incident. If not, go to SO 2.3.3.to continue investigation and diagnosis of the Incident.	Incident Analyst
SO 2.3.11	Reassign Incident to Coordinator	The Incident Analyst reassigns the incident to the Incident Coordinator if no resolution can be found. The analyst also provides information on the current status, work performed on the Incident, and information on reassignment. The Incident Coordinator can decide whether to escalate the incident, reassign the incident, or close the incident.	Incident Analyst
SO 2.3.12	Search Collect information	The Incident Analyst searches for information to provide the requested information to the User.	Incident Analyst
SO 2.3.13	Document Resolution/Workaround	The Incident Analyst documents the solution or workaround in the incident.	Incident Analyst

Incident Resolution and Recovery (process SO 2.4)

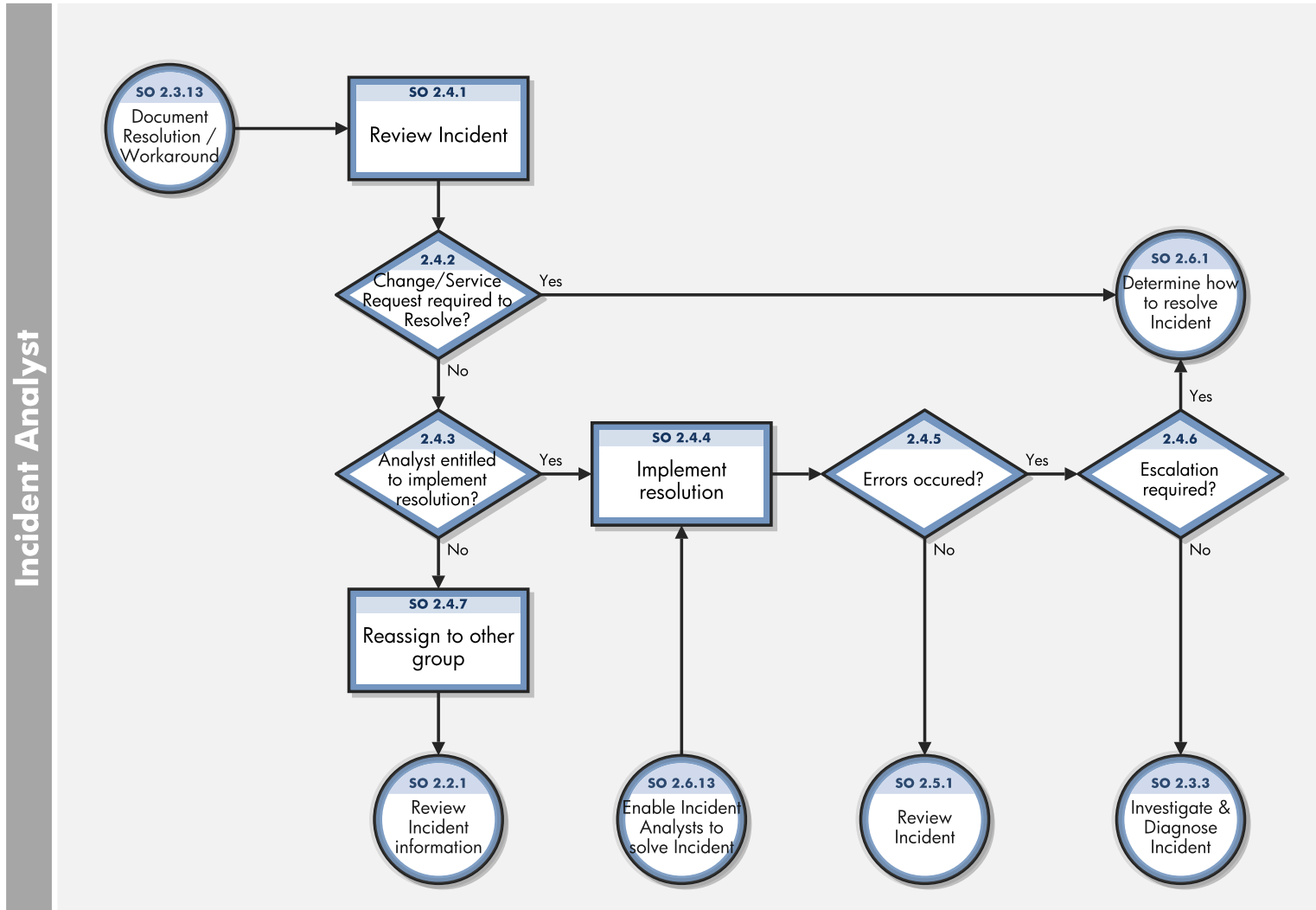
As part of the Incident Resolution and Recovery process, the Incident Analyst identifies and evaluates potential resolutions before those resolutions are applied and escalates incidents as necessary. The Incident Analyst may escalate an incident to the Incident Coordinator, including those incidents 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.

Incident Resolution and Recovery workflow is illustrated in the following figure:



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/ Service Request required to Resolve?	The Incident Analyst determines whether the resolution provided needs to be implemented by using a Change or Service Request. If yes, go to SO 2.6.1 for the Incident Coordinator to determine how to resolve the Incident. If not, go to SO 2.4.3 to determine whether the Analyst is entitled to implement the resolution.	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 tasks can be created for resolution implementation if required.	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 2.5.1.	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 or applicable vendor that can implement the solution.	Incident Analyst

Incident Review and Closure (process SO 2.5)

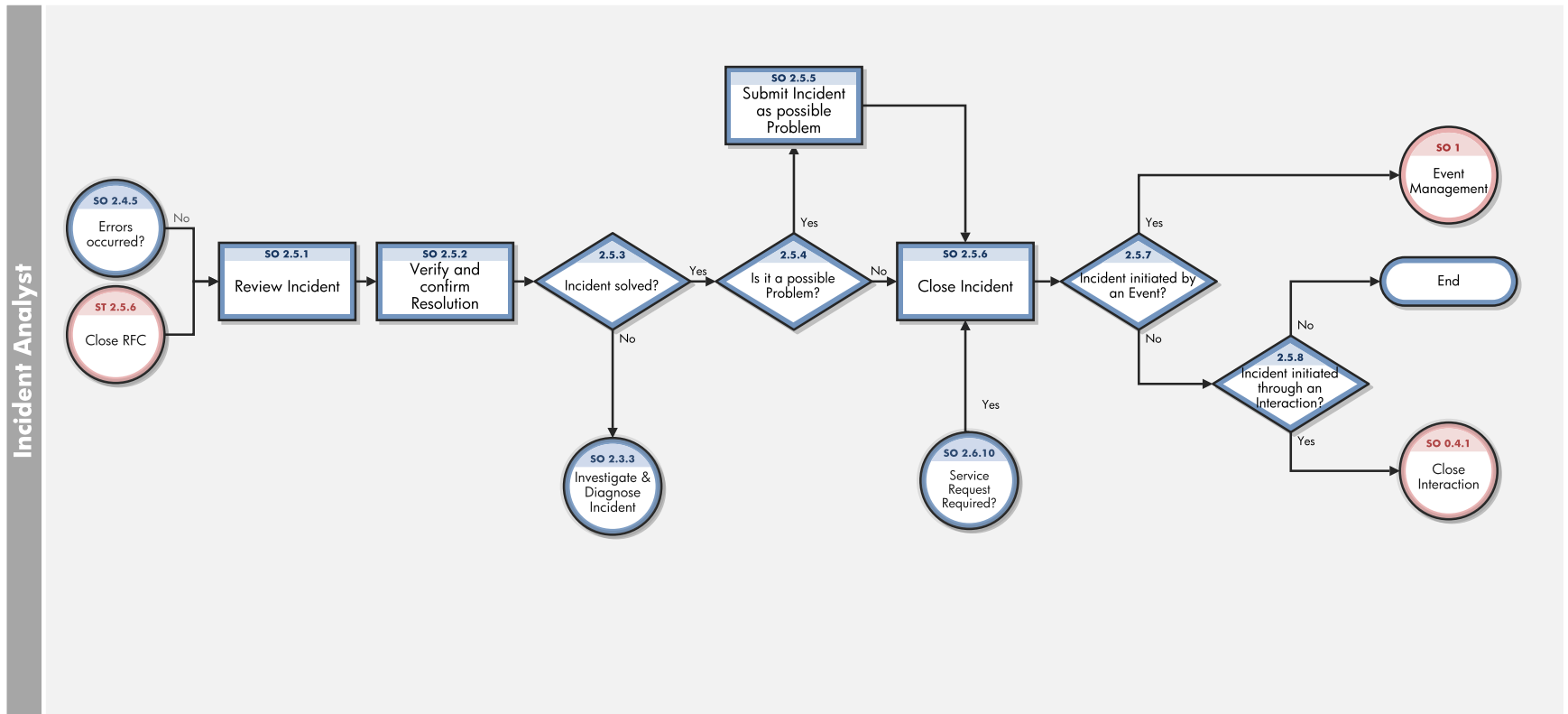
The Incident Review and Closure process includes many steps to verify the success of implemented solutions and to verify that incidents are accurate and complete.

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, the missing information must be added so that the incident 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.

Incident Closure workflow is illustrated in the following figure:



Incident Review and 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 2.3.3.	Incident Analyst
SO 2.5.4	Is it a possible Problem?	If the incident can be a possible problem, it is marked as possible problem and closed. Else the incident is closed without being marked as a possible problem.	Incident Analyst
SO 2.5.5	Submit Incident as possible Problem	The Incident Analyst submits the incident to Problem Management as a possible problem by checking the option to mark the Incident as a problem candidate.	Incident Analyst
SO 2.5.6	Close Incident	The Incident Analyst closes the incident and selects the applicable resolution code.	Incident Analyst
SO 2.5.7	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 2.5.8.	Incident Analyst
SO 2.5.8	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

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.

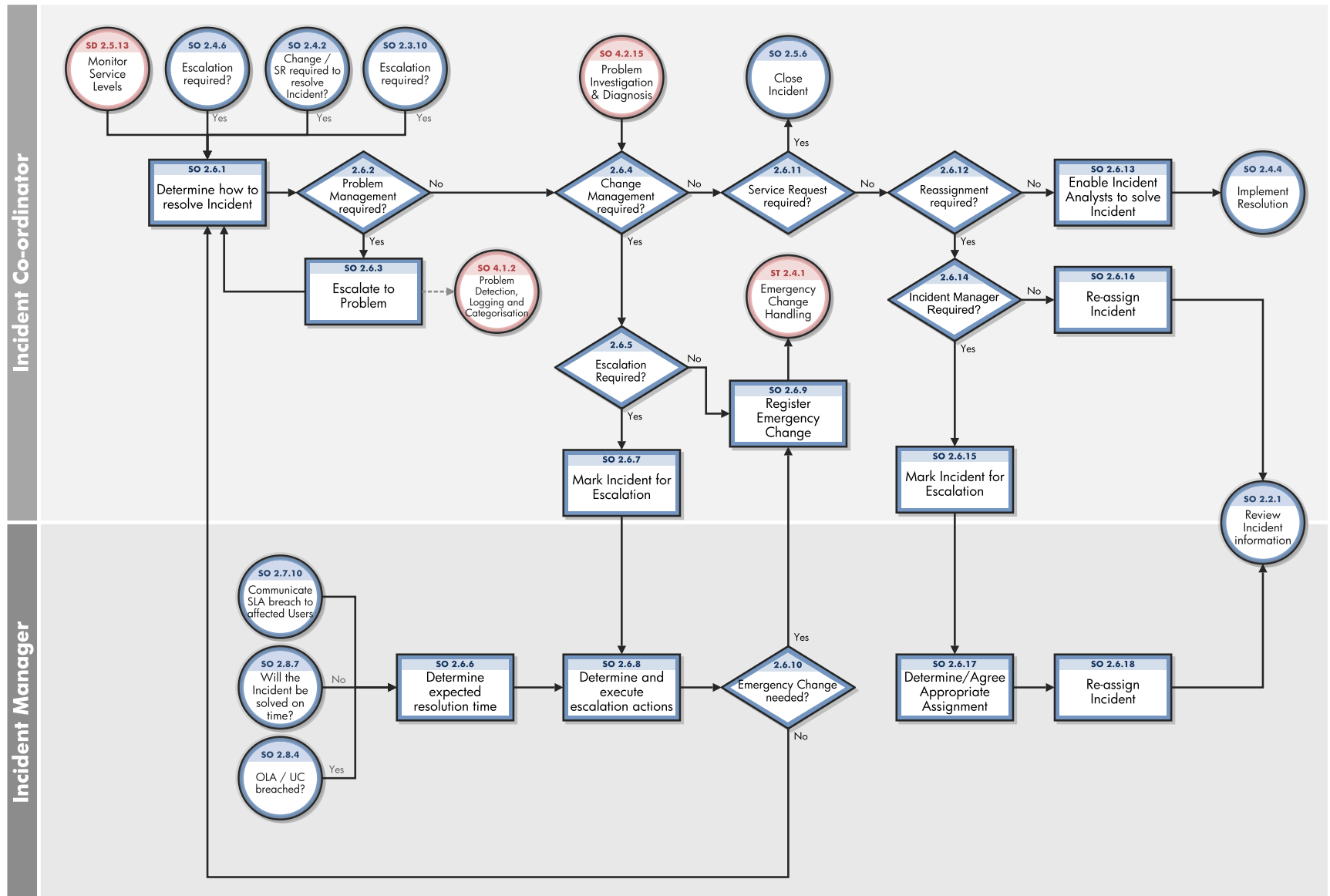
Incidents are escalated when the Incident Investigation and Diagnosis process or Incident Resolution and Recovery process exceeds SLA targets or if these targets are likely not to be met. If the steps to resolve an incident are taking too long or proving too difficult, the Incident Coordinator determines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

Incident Escalation workflow is illustrated in the following figure:



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	Problem Management required?	Is problem management required to solve the incident? If yes, continue with SO 2.6.3. If no, go to SO 2.6.4.	Incident Coordinator
SO 2.6.3	Escalate to Problem	Go to SO 2.6.1 to determine how to resolve the Incident.	Incident Coordinator
SO 2.6.4	Change Management required?	Is a change is required to solve the incident? If yes, continue with SO 2.6.5. If no, go to SO 2.6.11.	Incident Coordinator
SO 2.6.5	Escalation required?	Determine whether escalation is required to the Incident Manager to review what action to take with the Change Request. If yes go to SO 2.6.7 to mark the Incident for escalation. If not, go to SO 2.6.9 to Register Emergency Change	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	Mark Incident for Escalation	Mark Incident for Escalation The Incident Coordinator checks the Escalation checkbox in the incident record and marks the Incident for Escalation. A notification is sent to the Incident Manager informing him/her of escalation.	Incident Coordinator
SO 2.6.8	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

Incident Escalation process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.6.9	Register emergency change	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	Emergency change needed?	If yes, go to SO 2.6.9. If no, go to SO 2.6.1.	Incident Manager
SO 2.6.11	Service Request required?	If yes, close the Incident. If not, go to SO 2.6.12.	Incident Coordinator
SO 2.6.12	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 2.6.14. If no, go to SO 2.6.13.	Incident Coordinator
SO 2.6.13	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 2.6.14	Incident Manager required?	Escalation may be required for the Incident Manager to agree the appropriate assignment for the Incident. This may be required where there is a dispute over which group should take ownership of the Incident. If the Incident Manager must get involved, go to SO 2.6.15. If not, go to SO 2.6.16.	Incident Coordinator
SO 2.6.15	Mark Incident for Escalation	The Incident Coordinator checks the Escalation checkbox in the incident record and marks the Incident for Escalation. A notification is sent to the Incident Manager informing him/her of escalation. Then go to SO 2.6.17.	Incident Coordinator
SO 2.6.16	Reassign incident	The Incident Coordinator reassigns the incident to another 2nd-line or 3rd-line support group.	Incident Coordinator

Incident Escalation process, continued

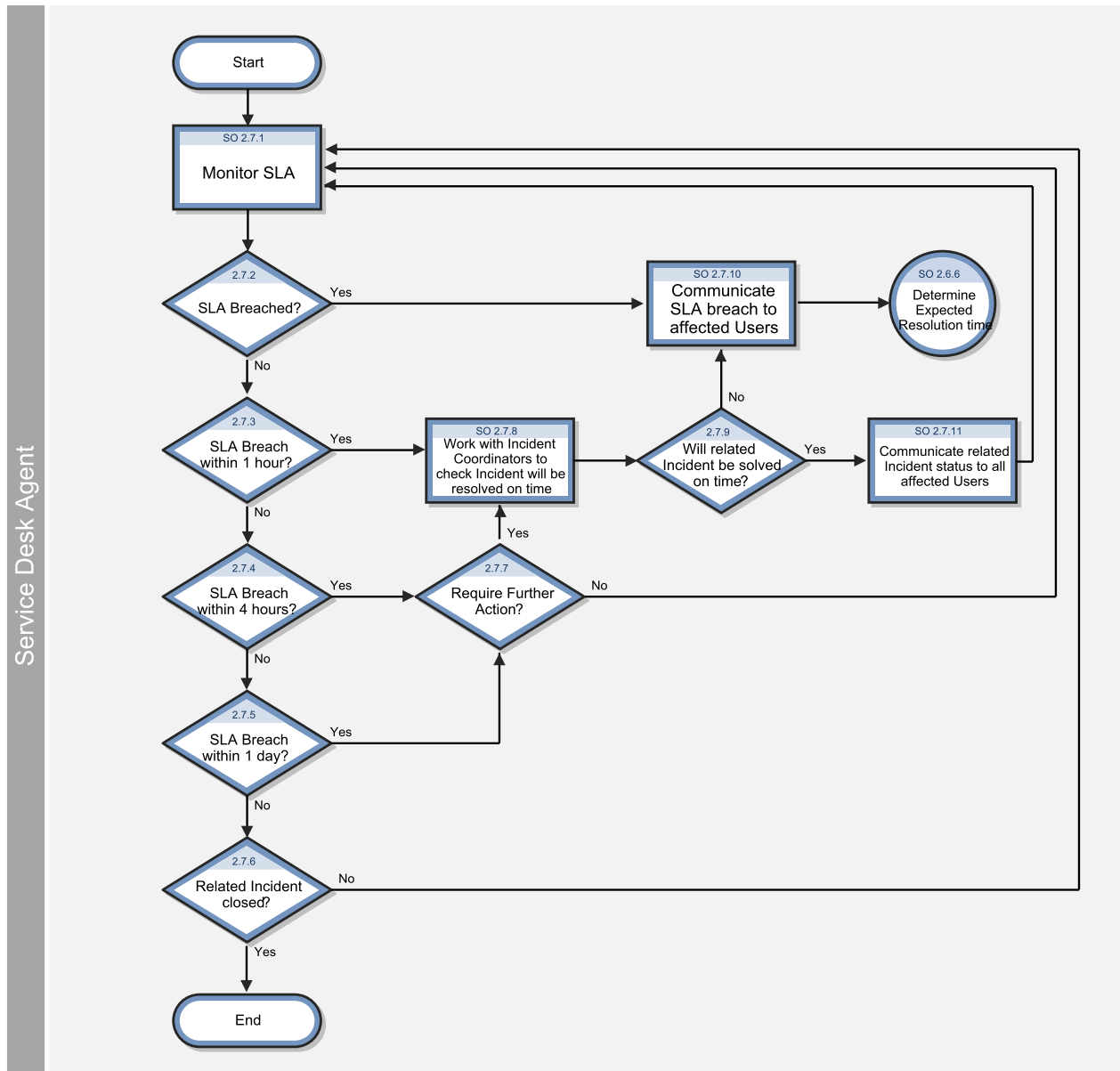
Process ID	Procedure or Decision	Description	Role
SO 2.6.17	Determine/ Agree appropriate assignment	The Incident Manager reviews the Incident to determine the appropriate Assignment Group based on the skills/ knowledge or permissions required to resolve the Incident.	Incident Manager
SO 2.6.18	Reassign 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.

SLA Monitoring workflow is illustrated in the following figure:



SLA Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 2.7.1	Monitor SLA	The Service Desk Agent monitors the SLA.	Service Desk Agent
SO 2.7.2	SLA breached?	Has the SLA target date/time been exceeded for this interaction? If yes, go to SO 2.7.10, and then start the Incident Escalation process. If no, go to SO 2.7.3.	Service Desk Agent
SO 2.7.3	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 2.7.8. If no, go to SO 2.7.4.	Service Desk Agent
SO 2.7.4	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 2.7.5.	Service Desk Agent
SO 2.7.5	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 2.7.7. If no, go to SO 2.7.6.	Service Desk Agent
SO 2.7.6	Related incident closed?	If yes, no further action is required. If no, go to SO 2.7.1.	Service Desk Agent
SO 2.7.7	Request further action?	Review the Incident and determine whether further action is required to ensure that it will be resolved within the SLA target date/time. If yes, go to SO 2.7.8 to work with the Incident Coordinators) to check the Incident will be resolved on time. If not, go to SO 2.7.1 to continue to monitor the SLA.	Service Desk Agent
SO 2.7.8	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

SLA Monitoring process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.7.9	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 2.7.11. If no, go to SO 2.7.10, and then escalate the incident.	Service Desk Agent
SO 2.7.10	Communicate SLA breach to affected Users	Identify which Users or user groups are affected by the SLA breach. Send a communication bulletin to inform all affected Users.	Service Desk Agent
SO 2.7.11	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

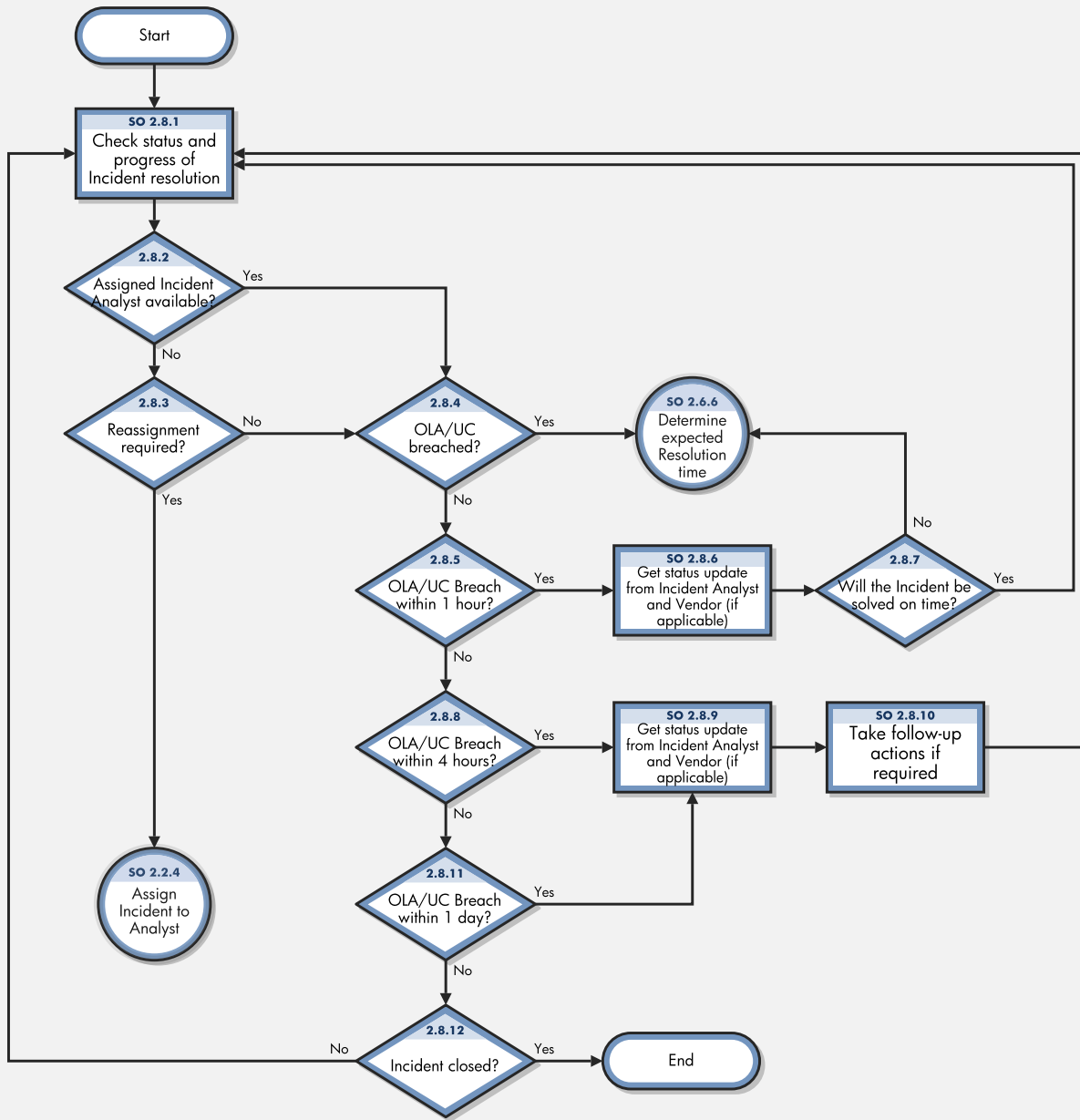
OLA and UC Monitoring (process SO 2.8)

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.

OLA and UC Monitoring workflow is illustrated in the following figure:



OLA and UC Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 2.8.1	Check status and progress of Incident resolution	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. If the Incident need to be assigned, SO 2.8.3. If not, go to SO 2.8.4.	Incident Coordinator
SO 2.8.3	Reassignment required?	If yes, go to SO 2.2.4. If no, go to SO 2.8.4.	Incident Coordinator
SO 2.8.4	OLA or UC breached?	If yes, start the Incident Escalation process (SO 2.6.6). If no, go to SO 2.8.5.	Incident Coordinator
SO 2.8.5	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 2.8.1. If no, go to SO 2.6.6 to determine the expected resolution time.	Incident Coordinator
SO 2.8.8	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

OLA and UC Monitoring process, continued

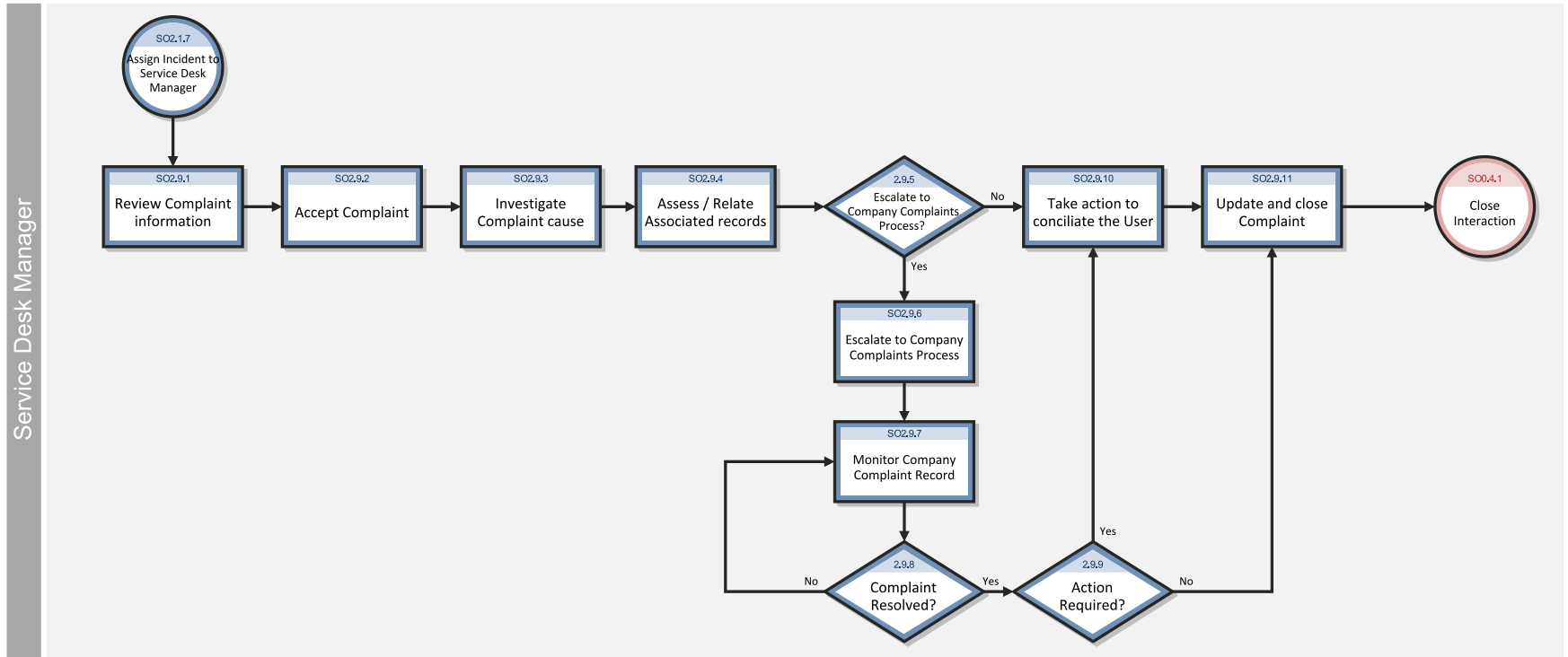
Process ID	Procedure or Decision	Description	Role
SO 2.8.10	Take follow-up actions if required	The Incident Coordinator determines whether follow-up actions are required to resolve the incident according to the OLA/UC. If required, the Incident Coordinator performs the required actions.	Incident Coordinator
SO 2.8.11	OLA/UC breach within 1 day?	If yes, go to SO 2.8.9. If no, go to SO 2.8.12.	Incident Coordinator
SO 2.8.12	Incident closed?	If yes, no further action is required. If no, go to SO 2.8.1.	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 with the agreed on details, and then closes the incident. You can see the details of this process in the following figure and table.

Complaint Handling workflow is illustrated in the following figure:



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 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	Assess/ Relate associated records	The Service Desk Manager assesses the associated records and relates them to existing records if necessary.	Service Desk Manager
SO 2.9.5	Escalate to company complaints process?	The Service Desk Manager assesses the complaint and determines whether it is within the scope of the Company Complaints Process. If escalation is necessary, go to SO 2.9.6. If not, go to SO 2.9.10.	Service Desk Manager
SO 2.9.6	Company complaints process	The Service Desk Manager escalates to have the complaint registered in the Company Complaints process and updates the Incident record.	Service Desk Manager
SO 2.9.7	Monitor company complain record	The Service Desk Manager monitors the complaint through the company complaint process.	Service Desk Manager
SO 2.9.8	Complaint resolved?	If the complaint is resolved, continue to SO 2.9.9. If not, go to SO 2.9.7.	Service Desk Manager

Complaint Handling process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.9.9	Action required?	If the complaint has been resolved but further action must be taken, go to SO 2.9.10. If no further action is required, go to SO 2.9.11.	Service Desk Manager
SO 2.9.10	Take action to conciliate the user	The Service Desk Manager contacts the user to solve the user's issue and tries to reach an agreement.	Service Desk Manager
SO 2.9.11	Update and close complaint	The Service Desk Manager updates the incident with the agreed on details and closes the incident.	Service Desk Manager

Chapter 10

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" below](#)
- ["Categorize incident form" on page 143](#)
- ["Investigate incident form" on page 143](#)
- ["Recover incident form" on page 144](#)
- ["Review incident form" on page 145](#)
- ["Incident Management form details" on page 146](#)

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.

Incident escalated from Service Desk is illustrated in the following screenshot:

Incident

Title: Desktop reboots with BIOS message CPU temperature critical
 Description: Critical CPU temperature causes frequent reboots

Incident ID: IM10152
 Status: Open
 Phase: Logging

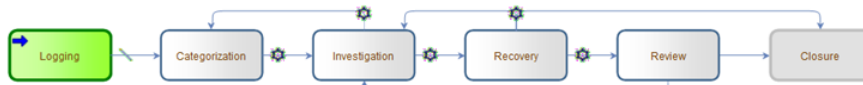
Affected Service: MyDevices
 Affected CI: adv-afr-desk-105
 CI is operational (no outage)

Outage Start Time:
 Outage End Time:

Category: incident
 Subcategory: performance
 Area: performance degradation

Impact: 4 - User
 Urgency: 3 - Average
 Contact Person: BELL, WILL
 Location: advantage/North America

Workflow



After saved, the incident enters Categorization phase which is illustrated in the following screenshot:

Incident - IM10152

Title: Desktop reboots with BIOS message CPU temperature critical
 Description: Critical CPU temperature causes frequent reboots

Incident ID: IM10152
 Status: Categorize
 Phase: Categorization

Affected Service: MyDevices
 Affected CI: adv-afr-desk-105
 CI is operational (no outage)

Outage Start Time: 06/10/13 22:13:25
 Outage End Time:

Requested By: falcon
 Contact Person: BELL, WILL
 Location: advantage/North America

Major Incident:
 Escalated:

Categorization and Assignment

Tasks

Impacted Services

Workflow

Proposed Solution

Related Records - (1)

Link Type:

ID	Type	Phase	Status	Title
SD10337	Escalate From	Categorization	Categorize	Desktop reboots with BIOS message CPU temperature critical

Categorize incident form

The Incident Coordinator uses the incident categorization form to review the information, and then categorize the incident, set expected resolution time, and assign the incident to an Incident Analyst in the appropriate support group.

Incident - IM10152

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10152	Requested By:	falcon
Status:	* Assign	Contact Person:	BELL, WILL
Phase:	Categorization	Location:	advantage/North America
Affected Service:	* MyDevices	Major Incident:	<input type="checkbox"/>
Affected CI:	adv-afr-desk-105	Escalated:	<input type="checkbox"/>
	<input type="checkbox"/> CI is operational (no outage)		
Outage Start Time:	06/10/13 22:13:25		
Outage End Time:			

Category and Assignment

Category:	incident	Impact:	* 4 - User
Subcategory:	* performance	Urgency:	* 3 - Average
Area:	performance degradation	Priority:	3 - Average
Assignment Group:	* Hardware	Expected Resolution Time:	06/15/13 00:00:00
Assignee:	* IncidentAnalyst		

Investigate incident form

The Incident Analyst uses the incident investigation 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.

Incident - IM10152

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10152	Requested By:	falcon
Status:	* Work In Progress	Contact Person:	BELL, WILL
Phase:	Investigation	Location:	advantage/North America
Affected Service:	* MyDevices	Major Incident:	<input type="checkbox"/>
Affected CI:	adv-afr-desk-105	Escalated:	<input type="checkbox"/>
	<input type="checkbox"/> CI is operational (no outage)		
Outage Start Time:	06/10/13 22:13:25		
Outage End Time:			

⊕ Categorization and Assignment

⊕ Tasks

⊕ Impacted Services

⊕ Proposed Solution

Problem Candidate:

Solution:

Recover incident form

The Incident Analyst tries to apply the resolution to the incident after diagnosis. Based on the nature of the resolution, the Incident Task, or the Change Management, Problem Management or vendor support is requested for assistance for the resolution.

Incident - IM10152

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10152	Requested By:	falcon
Status:	* Work In Progress	Contact Person:	BELL, WILL
Phase:	Recovery	Location:	advantage/North America
Affected Service:	* MyDevices	Major Incident:	<input type="checkbox"/>
Affected CI:	adv-afr-desk-105	Escalated:	<input type="checkbox"/>
	<input type="checkbox"/> CI is operational (no outage)		
Outage Start Time:	06/10/13 22:13:25		
Outage End Time:			

Categorization and Assignment

Tasks

Impacted Services

Proposed Solution

Problem Candidate:

Solution:

1. Change the position of the box so the outlet for air wasnt blowing to the wall
2. Clean the dusty PC: the motherboard, the air fans for the outlets, CPU fan, and the all the cards
3. Open up the box to let more cool air flow in
4. Install a software monitoring tool to monitor the CPU temperature

Review incident form

The Incident Coordinator verifies the incident resolution with the requester. If the requester is not satisfied with the resolution, the Incident Coordinator can reassign, escalate or close the incident. If the requester is satisfied with the resolution, the Incident Coordinator then close the Incident ticket after reviewing whether it is a problem candidate.

Incident - IM10152

Title: * Desktop reboots with BIOS message CPU temperature critical
 Description: * Critical CPU temperature causes frequent reboots

Incident ID: IM10152
 Status: * Resolved
 Phase: Review

Requested By: falcon
 Contact Person: BELL, WILL
 Location: advantage/North America

Affected Service: * MyDevices
 Affected CI: adv-afr-desk-105
 CI is operational (no outage)

Major Incident:
 Escalated:

Outage Start Time: 06/10/13 22:13:25
 Outage End Time:

⊞ Categorization and Assignment

⊞ Tasks

⊞ Impacted Services

⊞ Recovery Action

Problem Candidate:

Solution:

1. Change the position of the box so the outlet for air wasnt blowing to the wall
2. Clean the dusty PC: the motherboard, the air fans for the outlets, CPU fan, and the all the cards
3. Open up the box to let more cool air flow in
4. Install a software monitoring tool to monitor the CPU temperature

Incident Management form details

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

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

Incident Management form details

Label	Description
Incident ID	The system-generated unique ID for this incident.
Title	<p>A short description that summarizes the incident. This field is prepopulated with data from an escalated interaction.</p> <p>This is a required field.</p>
Description	<p>A detailed description of the incident. This field is prepopulated with data from an escalated interaction.</p> <p>This is a required field.</p>
Phase	<p>This is a system-generated field.</p> <p>These phases are available out-of-box:</p> <ul style="list-style-type: none">• Logging• Categorization• Investigation• Recovery• Review• Closure

Incident Management form details, continued

Label	Description
Status	<p>Displays the status of the incident.</p> <p>These statuses are available out-of-box:</p> <ul style="list-style-type: none"> • Open — The incident has been opened but it is not currently being worked on. • Categorize – The incident has been categorized • Assign – The incident has been assigned to appropriate resource • 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 Evidence — You need evidence from the customer or vendor • Pending Other — You need something from an outside source other than customer or vendor. • Suspended — Customer has agreed to suspend the incident for a time; the incident will not appear in your Inbox for that period. • Resolved — There is a resolution, but it has not yet been verified by the customer. • Closed — The incident has been resolved and the customer agrees.
Affected Service	<p>The service affected by this incident. This field is populated with data from the interaction record.</p> <p>See "Service Desk Interaction Management form details" on page 84 for additional information.</p> <p>This is a required field.</p>
Affected CI	<p>The configuration item (CI) that is affecting the service negatively. This field is populated with data from the interaction record.</p> <p>See "Service Desk Interaction Management form details" on page 84 for additional information.</p> <p>This field includes a hover-over form that displays Critical CI and Pending Change check boxes to indicate whether or not these attributes apply to the CI.</p>

Incident Management form details, continued

Label	Description
CI is operational (no outage)	This field indicates that the item is currently operational and that there is no outage if selected (set to true). 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.
Outage Start	The date and time when the outage started. The outage start and outage end times are used to measure the availability for the Service Level Agreements (SLAs). If the CI is flagged as down, availability SLAs start counting against the CI. The default availability value is the incident open and close times, but you should change this value 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.
Outage End	The date and time when the outage ended. The outage start and outage end times are used to measure the availability for the SLAs. If the CI is flagged as down, availability SLAs start counting against the CI. The default availability value is the incident open and close times, but you should change this value 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.
Category	<p>This field describes the type of incident, based on ITIL service-centric processes. This field is prepopulated with data from the escalated interaction.</p> <p>This is a required field. A workflow is bound to a category. You must select a category before open an incident form, if incident is not opened from escalation and there is no default category specified.</p> <p>If required, the Incident Coordinator, Incident Manager, and Incident Analyst can update this field and the related subcategory and area fields for incidents assigned to them. This field is read-only, to update the category, they need to click More > Change Category menu option.</p> <p>These categories are available for Incident out-of-box:</p> <ul style="list-style-type: none"> • Incident • Complaint • Request for administration • Request for information

Incident Management form details, continued

Label	Description
Subcategory	<p>This field is prepopulated with data from an escalated interaction. The subcategory selections depend on the category.</p> <p>This is a required field when phase starts from Categorization.</p> <p>The out-of-box data is the same as in Interaction Management, but can be different. For additional information, see "Service Desk Interaction Management form details" on page 84 and "Interaction categories" on page 95.</p>
Area	<p>The third level of classifying an interaction, mainly used for reporting purposes. This field is prepopulated with data from an escalated interaction.</p> <p>Service Manager displays different lists of areas, depending on the subcategory selected. For more information on categories and the areas and subareas associated with them, see "Interaction categories" on page 95.</p> <p>The out-of-box data is the same as in Interaction Management, but can be different. For additional information, see "Service Desk Interaction Management form details" on page 84.</p>
Impact	<p>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.</p> <p>These impacts are available out-of-box:</p> <ul style="list-style-type: none"> • Enterprise • Site/Dept • Multiple Users • User
Urgency	<p>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 "Service Desk Interaction Management form details" on page 84.</p>
Priority	<p>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.</p>
Major Incident	<p>If selected (set to true), this field indicates that the issue is a major issue, which requires to inform the specified Incident Manager.</p>

Incident Management form details, continued

Label	Description
Escalated	If selected (set to true), this field indicates that the incident needs to be escalated to Incident Manager, and possibly additional escalation teams also need to be aware of.
Requested By	The name of operator who opened the Incident ticket. This field is populated with the current operator.
Contact Person	This field contains the contact name related to the company 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. This field is prepopulated with data from an interaction when a user opens an incident from an interaction.
Location	The location for which the incident has been reported. This field is for informational purposes only. Location data is customer and implementation specific.

Incident Management form details, continued

Label	Description
Categorization and Assignment section > Assignment Group	<p>The support group assigned to work on this incident. The affected service or CI 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 or CI specified in the Config admin group field. When you escalate an interaction to an incident, the assignment group is prepopulated, based on the CI or service (if no CI selected, then based on selected service) selected in the interaction. You can change the assignment group, if necessary.</p> <p>The out-of-box data consists of default assignment groups for use as examples of types of assignment groups.</p> <div data-bbox="521 835 1370 947" style="background-color: #f0f0f0; padding: 5px;"> <p>Tip: You may want to adapt the sample assignment groups to meet your own needs.</p> </div> <p>These assignment groups are available out-of-box:</p> <ul style="list-style-type: none"> • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager <p>This is a required field.</p>

Incident Management form details, continued

Label	Description
Categorization and Assignment section > 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.
Categorization and Assignment section > Expected Resolution Time	The Incident Coordinator can use this field to set an expectation for incident resolution time.
Workflow section	Workflow section displays a figure of incident workflow. It also indicates the current phase which the incident is in, and traces the phase transition history.
Tasks section	<p>The user can add tasks whenever an incident is in a phase. Every task has to be finished before close the incident. To add a new task, click the Tasks section, and then click the Link New Task button. Service Manager provides a quick view of some of the most important fields in the task in the Tasks section. The data displayed includes the following information:</p> <ul style="list-style-type: none"> • Task ID • Status • Phase • Priority • Title
Activities > Vendor	The name of the vendor the incident is assigned to. Used when a vendor needs to be involved in fixing the incident.
Activities > Vendor Ticket	This number refers to the incident number from the vendor's logging system. This is an informational field for reference only. This field is only visible when incident status is Pending Vendor.

Incident Management form details, continued

Label	Description
Related Records section > Link Type	Specify a relation type between problem and target ticket. These link type groups are available out-of-box: <ul style="list-style-type: none"> • Caused By Incidents • Caused Incidents • Caused By Changes • Related Interactions • Related Problems • Related Quotes
Related Records section > Link Existing/New Record button	After select a link type, uses these two buttons to associate the incident with target ticket, or create a new target ticket and associate with this incident.
Related Records section > All Related Records table	Information of all related records of this problem is displayed in this table. The data displayed includes the following information: <ul style="list-style-type: none"> • ID • (Relation) Type • Phase • Status • Title
Related Records section > Unlink Record button	If you want to disassociate the incident with another ticket, select the related ticket from All Related Records table, and click this button to unlink these two tickets.
Proposed Solution/Recovery Action section > Solution	Provides a description of the solution for the incident.

Incident Management form details, continued

Label	Description
Proposed Solution/Recovery Action section > Problem Candidate	<p>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 should have been created, or the incident should have been associated with other problems. This field is only enabled for users who have Expert rights. This capability is specified on the Incident Management Security Role area. When the Problem Management Candidate field is checked for the incident, the incident 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.</p>
Closure Code	<p>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.</p> <div data-bbox="521 842 1370 953" style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Tip: You may want to tailor these options to match your business needs.</p> </div> <p>These closure codes are available out-of-box:</p> <ul style="list-style-type: none"> • 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 • No Fault Found • No User Response • Resolved Successfully • Diagnosed Successfully
Completion Comments	<p>This field is to document additional comments to close the incident.</p>

Incident Management form details, continued

Label	Description
Affected Services	<p>This section provides a list of affected services for the incident. 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 is locked, the routine reschedules the schedule record for 5 minutes later.</p>
SLA > Response Time Objectives	<p>This subsection 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.</p>
SLA > Uptime Objectives	<p>This subsection displays uptime availability data for the SLOs related to the incident.</p> <p>The data displayed includes the following information:</p> <ul style="list-style-type: none"> • Status • SLO name • Required Monthly Uptime (%) • Withdrawn by User • Current Uptime this Month (%) • Next Expiration • Affected CI • SLO ID <p>Similar information is available for interactions, problems, and changes.</p>

Incident Management form details, continued

Label	Description
SLA > Max Duration Objectives	<p>This subsection displays duration availability data for the SLOs related to the incident.</p> <p>The data displayed includes the following information:</p> <ul style="list-style-type: none">• Status• SLO name• Total outages this month• Average outage duration• Next expiration• Affected CI• SLO ID <p>Similar information is available for interactions, problems, and changes.</p>
SLA > Upcoming Alerts	<p>This subsection displays all upcoming SLA alerts to help users prioritize the incidents needing attention.</p> <p>The data displayed includes the following information:</p> <ul style="list-style-type: none">• Alert name• SLO name• Alert time <p>Note: For additional information, see the online Help topic, Service Level Agreement alerts.</p>

Chapter 11

Problem Management Overview

The HP Service Manager Problem Management application (Problem Management) supports the entire problem management process. Problem Management provides comprehensive problem management that enables 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 to implement the best practice guidelines for the problem management process in Problem Management.

This section includes the following topics:

- ["Problem Management within the ITIL framework" below](#)
- ["The Problem Management application" on the next page](#)
- ["Problem management process overview" on page 160](#)
- ["Input and output of Problem Management" on page 164](#)
- ["Key Performance Indicators for Problem Management" on page 166](#)
- ["RACI matrix for Problem Management" on page 168](#)

Problem Management within the ITIL framework

The problem management process is described in ITIL's *Service Operation* document. The document describes problem management as the process by which the lifecycle of all problems is managed.

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 similar incidents in the future, 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 the service operation process, and is based on incident history.

- Proactive problem management identifies and solves issues and problems that are identified as known errors, before incidents occur. Reactive problem management is generally driven as part of the continual service improvement process.

By actively preventing incidents, instead of reacting to them, an organization provides better service and operates more efficiently.

Differences between Problem Management and Incident Management

Incident Management and Problem Management are separate, but closely-related, processes. Incident Management enables you to restore service to users, whereas Problem Management manages the lifecycle of all problems and enables you to identify and remove the underlying causes of incidents.

The Problem Management application

Problem Management 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. Additionally, Problem Management enables you to identify errors in IT infrastructure, record them, track the history, find resolutions for them, and prevent their recurrence.

Problem Management 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, the use of Problem Management reduces the volume of incidents, and saves time and money.

Problem Management workflows and categories

Problem Management comes with a single out-of-box workflow (the “Problem” workflow) for problems or known error records. This workflow is associated with a single out-of-box category (the “problem” category). The “Problem” workflow ensures that the problem workflow automatically conforms to the ITIL workflow.

If your business needs require changes to the out-of-box workflow, you can define new workflows. To do this, copy the out-of-box “Problem” workflow, add your own phases and transitions, and then associate the new workflow with the out-of-box “problem” category (or a new category). Each new category that you define enables you to associate a different workflow with a problem. If you define new categories, you can select one to be the default category for problems.

Problem tasks

Problem tasks have a single out-of-box task workflow (the “Problem Task” workflow) and four out-of-box task categories (the “Categorization,” “Investigation,” “Resolution,” and “Review” task categories). The four problem task categories are associated to the single workflow. You can define new workflows for problem tasks by copying and modifying the out-of-box workflow. You can also change the task categories or add other task categories. You can define unique task categories for the tasks that you assign to a problem.

Problem Management alerts

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

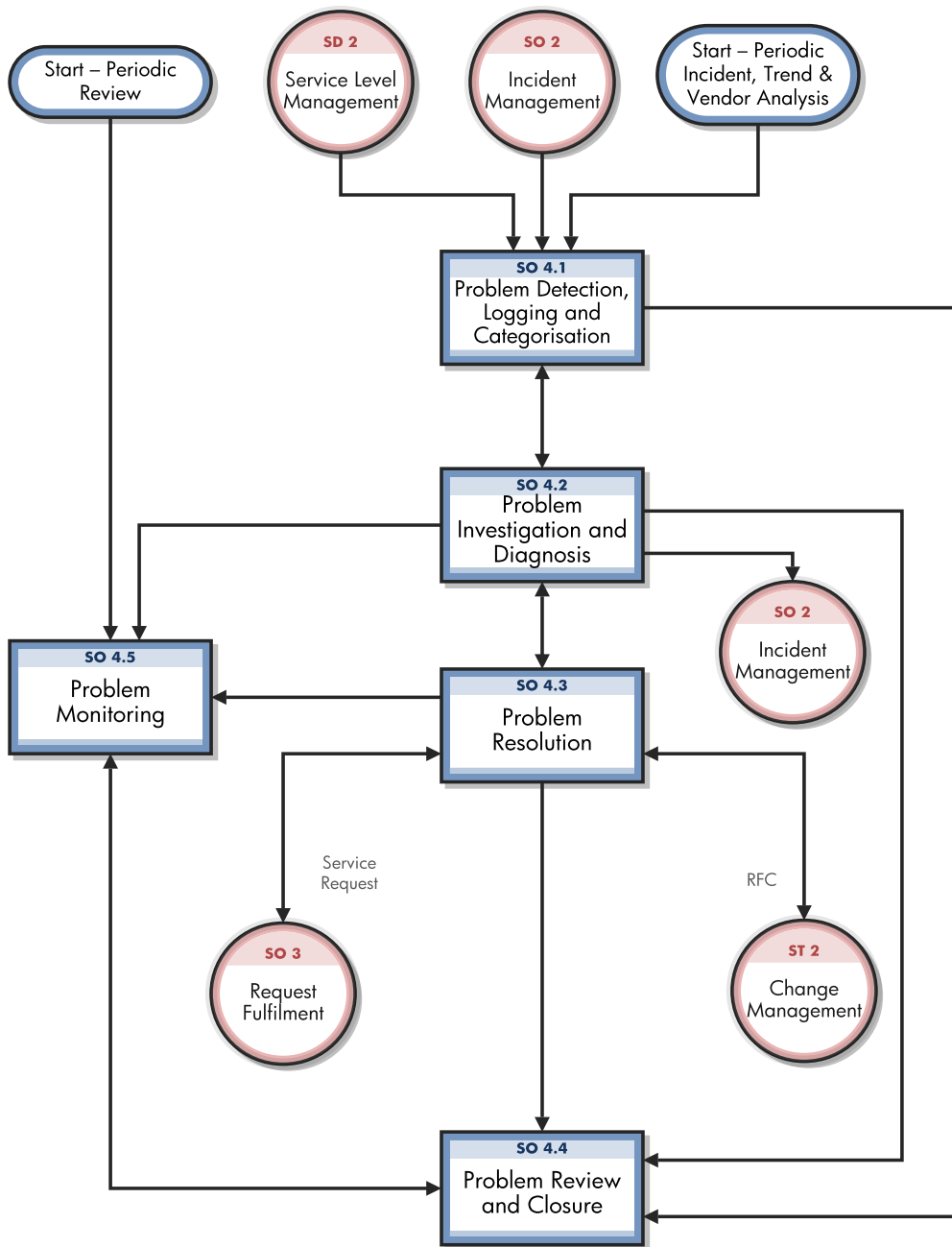
Problem management process overview

The problem management process includes the activities that are required to identify and classify problems, diagnose the root cause of incidents, and determine resolutions to related problems. The process ensures that the resolution is implemented through the appropriate control processes, such as change management.

Problem Management includes the activities that are required to prevent the recurrence or replication of incidents. It enables you to form recommendations for improvement, maintain problems, 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 the information that is given to customers for future use. This information reduces future information requests and helps to prevent incidents caused by lack of user knowledge and training.

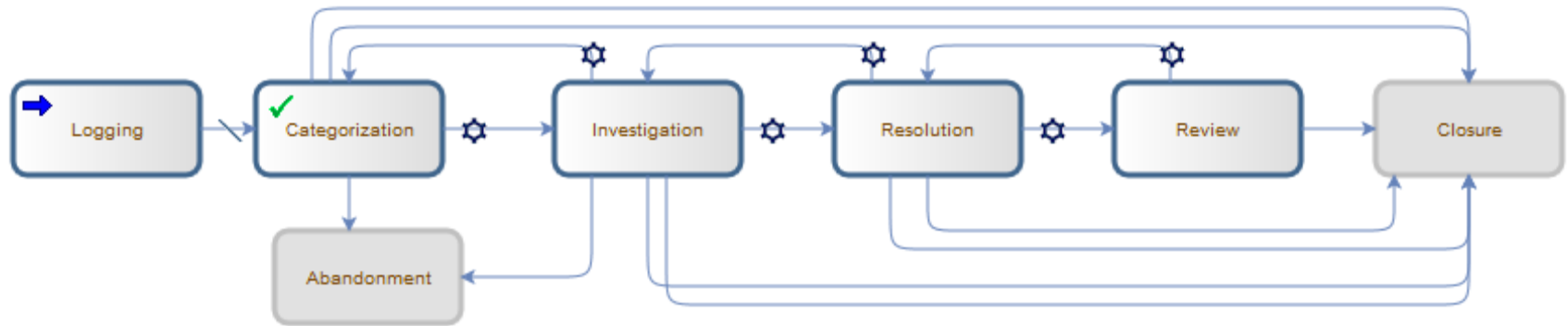
The following figure provides a general overview of the problem management processes and workflows. These workflows are described in detail in ["Problem Management Workflows" on page 169](#).



Problem management phases

Service Manager uses phases to describe the steps needed to resolve a problem. The phase also determines the forms users see, the actions users can manually trigger. In an out-of-box system, most of the phase transitions are triggered by change to the problem status.

The following figure shows the workflow phases for a problem.



Problem Management user roles

The following table describes the responsibilities of the Problem Management user roles.

Problem Management user roles

Role	Responsibilities
Problem Manager	<ul style="list-style-type: none">• Communicate with stakeholders if required• Inform the Change Manager if required• Defer problems if needed• Decide on investigation of problems• Register Request for Changes or Service Requests to solve problems• Validate proposed solutions to problems• Validate the outcome of closed changes and close problem• Validate that a problem is solved• Conduct problem review and document lessons learned• Close problem and inform stakeholders• Monitor the problem resolution progress and perform the required action
Problem Coordinator	<ul style="list-style-type: none">• Periodically perform analysis to see if new problems need to be registered• Register problems• Categorize and prioritize problems• Assign work to the Problem Analysts• Schedule the problem resolution• Coordinate root cause analysis and diagnosis

Problem Management user roles , continued

Role	Responsibilities
Problem Analyst	<ul style="list-style-type: none">• Investigate and diagnose assigned problems for workarounds and/or root causes• Review and accept or reject assigned errors problems or problem tasks• Investigate and diagnose assigned problems and propose solutions and workarounds• Identify known errors• Implement corrective actions

Input and output of Problem Management

Problems can be triggered and resolved in several ways. The following table outlines the input and output of the Problem Management process.

Input and output for Problem Management

Input to Problem Management	Output from Problem Management
<ul style="list-style-type: none"> • 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 a 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 <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ▪ Trend analysis and review of events (for example, performance events) ▪ Error logs • Configuration management 	<ul style="list-style-type: none"> • Problems • Known errors • Workarounds • Problem reports (for example, status updates, trends, and performance) <div data-bbox="955 573 1845 716" style="background-color: #f0f0f0; padding: 10px; margin-top: 20px;"> <p>Note: Information on workarounds, permanent fixes, or the progress of problems should be communicated to those who are affected and those who are required in order to support the affected services.</p> </div>

Input and output for Problem Management, continued

Input to Problem Management	Output from Problem Management
<ul style="list-style-type: none"> ▪ Configuration details and relationships (service model) • Change management <ul style="list-style-type: none"> ▪ RFC and change request status, approval and closure. • Security management <ul style="list-style-type: none"> ▪ Notification of potential security breaches that require resolution • Suppliers (external providers) • Notification of problems from suppliers/vendors 	

Key Performance Indicators for Problem Management

The Key Performance Indicators (KPIs) in the following table 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 KPIs. To visualize trend information, it is useful to display KPI data in graph form.

Problem Management KPIs

Title	Description
Average time to diagnose	The average time to diagnose problems and to pinpoint the root cause in a given time period.
Average time to fix	The average time to fix problem(s).
Number of new problems	The total number of problems recorded in a given time period.
Number of solved problems	The 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:

- The total number of problems recorded in a given period (as a control measure)
- The percentage of problems resolved within the SLA targets; also the percentage not resolved within the SLA targets
- The number and percentage of problems that exceed target resolution times
- The backlog of existing problems, and the growth trend of the backlog (that is, static, reducing, or increasing)
- The average cost of handling a problem
- The number of major problems, including opened, closed, and backlogged
- The percentage of major problem reviews successfully performed
- The number of known errors added to the known error Database (KEDB)
- The percentage accuracy of the KEDB (from audits of the database)
- The percentage of major problem reviews that were 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 that have a business impact
- Number of business disruptions caused by operational problems
- Percentage of problems recorded and tracked
- Percentage of problems that recur (within a time period), ranked by severity

- Percentage of problems resolved within the required time period
- Number of open, new, and closed problems, ranked by severity
- Average and standard deviation of the time lag between problem identification and resolution
- Average and standard deviation of the time lag between problem resolution and closure
- Average duration between the logging of a problem and the identification of the root cause
- Percentage of problems for which 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 the various teams or people that are responsible for delivering a project or operating a process. The matrix is especially useful for clarifying roles and responsibilities in cross-functional/departmental projects and processes. The following table displays the RACI matrix for Problem Management.

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	I	
SO 4.2	Problem Investigation and Diagnosis	A	C	R	
SO 4.3	Problem Resolution	A	C	R	R
SO 4.4	Problem Review and Closure	A/R	C		
SO 4.5	Problem Monitoring	A/R	C		

Chapter 12

Problem Management Workflows

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

Problem management includes the activities that are required to prevent the recurrence or replication of incidents. It enables you to form recommendations for improvement, maintain problems, 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 \(process SO 4.1\)" on the next page](#)
- ["Problem Investigation and Diagnosis \(process SO 4.2\)" on page 174](#)
- ["Problem Resolution \(process SO 4.3\)" on page 180](#)
- ["Problem Review and Closure \(process SO 4.4\)" on page 185](#)
- ["Problem Monitoring \(process SO 4.5\)" on page 190](#)

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 needs to be opened in order to investigate an existing or potential problem. This process can be started in response to a single incident, a series of related incidents, or a single interaction. The process may also result from the proactive investigation of a potential problem.

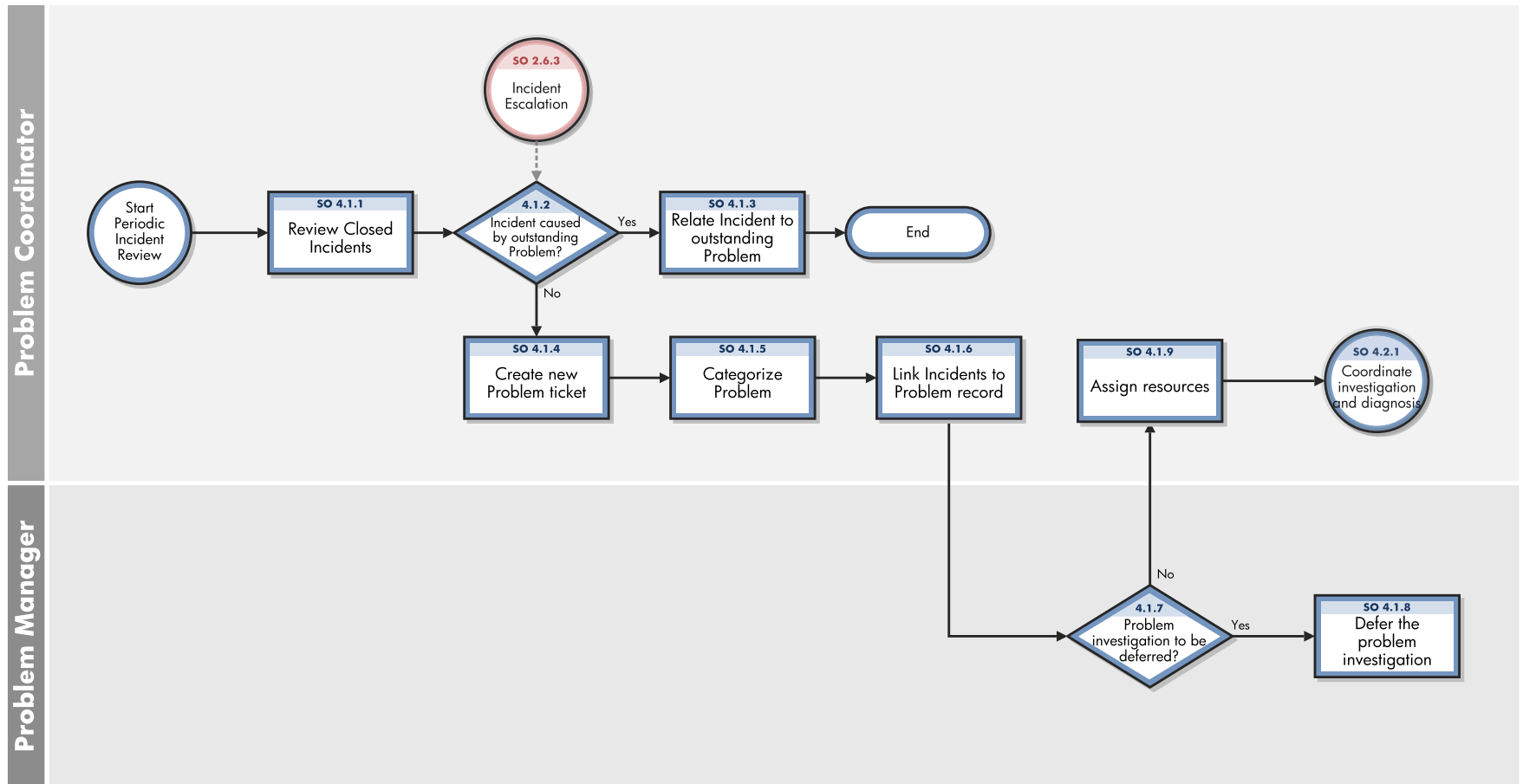
The Problem Detection, Logging, and Categorization process should include reference to information that assists analysis, such as:

- Asset and configuration
- Change management
- Published workaround information from suppliers
- Historical information about similar problems
- Monitoring event logs and other data collected by system management tools

The incident(s) that initiated the problem should be referenced, and relevant details copied from the incident(s) to the problem. If the Incident Analyst has identified a workaround or temporary fix, this should be included as well.

A problem ticket is created. All relevant details of the problem must be recorded so that an accurate historic record exists. Other details like impact and category of the problem are also identified.

The following figure illustrates the Problem Detection, Logging, and Categorization workflow:



Problem Detection, Logging, and Categorization process

Process ID	Procedure or Decision	Description	Role
SO 4.1.1	Review closed incidents	<p>Periodically, the Problem Coordinator must review the closed incidents to detect new problems or to match incidents to existing problems that have not been resolved. Analysis of incident data may reveal similar or reoccurring incidents, which means that a permanent fix must be found. Select incidents since the last review by using the following criteria:</p> <ul style="list-style-type: none"> • Major incidents (high impact) • Incidents resolved through a workaround or a temporary fix that is not matched to a problem. • Suspected problems (as identified by stakeholders) • Candidates for problems <p>All closed incidents that are not resolved through a permanent fix, temporary fix, or workaround must be matched to existing problems. Or, a new problem must be created. Incident management staff may have linked incidents to existing problems already (for example, if a workaround has been applied).</p>	Problem Coordinator
SO 4.1.2	Incident caused by outstanding problem?	<p>If the incident is caused by an outstanding problem, the workflow moves to SO 4.1.3. If the incident is not caused by an outstanding problem, the workflow moves 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. The incident count influences the prioritization of problems by indicating the frequency of occurrence and thus the business impact of this issue.</p>	Problem Coordinator
SO 4.1.3	Relate incident to outstanding problem	<p>If the incident is caused by an outstanding problem, the incident must be linked to the problem. If required, the problem is updated and the Problem Analyst is notified (for example, when a workaround has been applied).</p>	Problem Coordinator

Problem Detection, Logging, and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.1.4	Create new problem ticket	<p>Create a new problem ticket that captures all the relevant data, such as:</p> <ul style="list-style-type: none"> • User details • Configuration Item (CI) details • Date and time the problem was initially logged • Description • Details of all diagnostic or attempted recovery actions taken so far <p>The Problem Coordinator can estimate the resources and costs that are required to resolve a problem during any stage of the Problem lifecycle. These details are entered in the problem record, and are used to decide the next course of action for the ticket.</p>	Problem Coordinator
SO 4.1.5	Categorize problem	<p>The Problem Coordinator categorizes the problem into a specific domain (for example, hardware, software, or security).</p> <p>Problems can be categorized in the same way as incidents, so that the true nature of problems can be easily traced in the future, and meaningful management information can be obtained. Other information (such as the estimated cost and estimated effort) is entered, if it is available at this stage. These fields can be updated at a later stage if new information becomes available.</p> <p>If the problem is not categorized in the appropriate category, the Problem Coordinator can change the category, which initiates a new workflow.</p>	Problem Coordinator
SO 4.1.6	Link incidents to problem record	<p>The Problem Coordinator links all related incident records to the problem record. The Problem Coordinator also captures other information, such as the impact (from SLM), urgency, and subcategory of the problem.</p>	Problem Coordinator

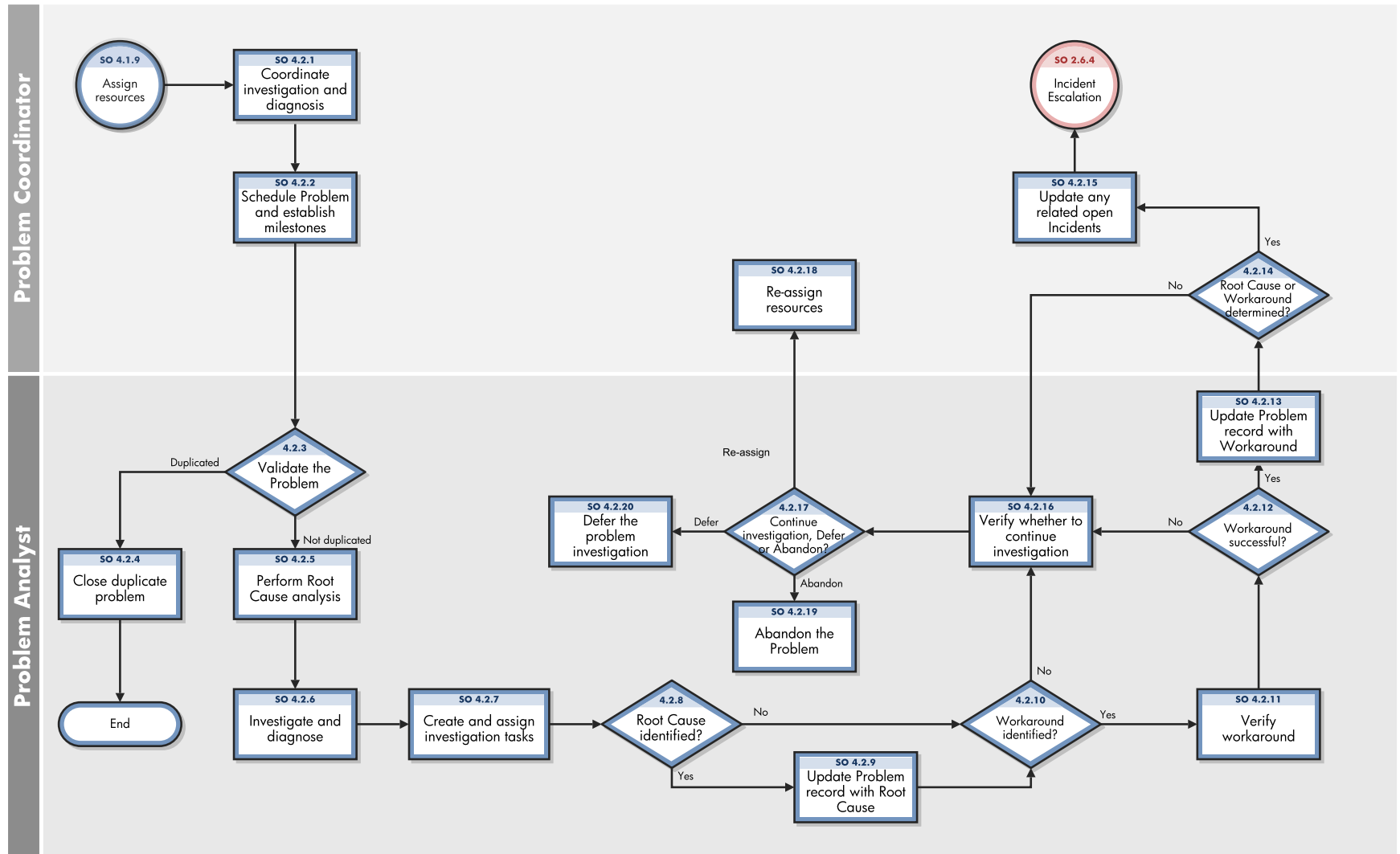
Problem Detection, Logging, and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.1.7	Problem investigation to be Deferred?	If the problem investigation must be deferred, move the problem to the appropriate status. If the problem investigation does not need to be deferred, go to SO 4.1.9.	Problem Manager
SO 4.1.8	Defer the problem investigation	<p>The Problem Manager defers the problem investigation for a specific period of time. The reason for deferring the problem is detailed in the ticket. Periodically, the Problem Manager reviews the deferred problems to determine the appropriate action.</p> <p>Reasons for deferring problem include the following:</p> <ul style="list-style-type: none">• The likelihood of recurrence is low• The cost of resolving the problem is very high• There is currently no plan to investigate the problem	Problem Manager
SO 4.1.9	Assign Resources	The Problem Coordinator determines the skills and personnel that are required to resolve the problem, and assigns personnel to resolve the problem.	Problem Coordinator

Problem Investigation and Diagnosis (process SO 4.2)

The Problem Investigation and Diagnosis process helps identify the root cause of the problem. Where appropriate, the problem management process should develop and maintain workarounds that enable the incident management process to help service restoration. Different specialists can be involved in this root cause analysis. If necessary, refer to external resources to verify whether the problem has already been identified and published by vendors. Decide the target dates for the problem investigation.

The following figure illustrates the Problem Investigation and Diagnosis workflow:



Problem Investigation and Diagnosis process

Process ID	Procedure or Decision	Description	Role
SO 4.2.1	Coordinate investigation and diagnosis	The Problem Coordinator verifies the schedules of resources, and assigns the resources to the problem resolution. The assigned resource starts their investigation. The Problem Coordinator coordinates the tasks that required to resolve the problem, and maintains communication with all stakeholders.	Problem Coordinator
SO 4.2.2	Schedule the problem and establish milestones	The Problem Coordinator estimates the cost and effort required to resolve the problem, and determines the target dates for the problem resolution milestones. Target dates are determined by the priority of the problem and by the impact of the problem on affected services. Additionally, this phase of planning considers whether an effective workaround or fix is available.	Problem Coordinator
SO 4.2.3	Validate the problem	The Problem Analyst ensures that the problem record is valid. The Problem Analyst determines whether the problem record is a duplicate or new problem. Then, the Problem Analyst continues with root cause analysis. If the problem is a duplicate, it is linked to the problem that it is a duplicated of, and the workflow moves to SO 4.2.5. If the problem is not a duplicate, the workflow moves to SO 4.2.4.	Problem Analyst
SO 4.2.4	Close duplicate problem	The Problem Analyst closes the problem as a duplicate, and enters the necessary closure comments into the ticket.	Problem Analyst

Problem Investigation and Diagnosis process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.2.5	Perform root cause analysis	<p>The Problem Analyst performs root cause analysis of the problem. Root cause analysis can include the following methods:</p> <ul style="list-style-type: none"> • Chronological Analysis • Pain Value Analysis • Kepner and Tregoe • Brainstorming • Ishikawa Diagrams • Pareto Analysis 	Problem Analyst
SO 4.2.6	Investigate and diagnose	<p>The Problem Analyst analyzes the known data to identify and isolate the root cause of the problem. If a potential root cause is identified, it is verified. If more resources are required to do this, they are requested through the Problem Coordinator, who requests them from the Problem Manager and Problem Coordinator.</p> <p>Additionally, the Problem Analyst tries to identify a workaround. Potential workarounds are tested to verify that they work. If successful, a workarounds is documented in the problem record. The same is intimated to Service Desk and Incident Analysts</p>	Problem Analyst
SO 4.2.7	Create and assign investigation tasks	<p>The Problem Analyst creates and assigns problem tasks to the resource who is responsible for root cause analysis. The Problem Analyst enters the due date for the assigned task. Additional resources (for example, suppliers and other specialists) can be used for this analysis. The Problem Analyst monitors the outstanding problem tasks.</p>	Problem Analyst
SO 4.2.8	Root cause identified?	<p>If the root cause is not identified, the Problem Analyst must determine whether there is a workaround for the problem.</p> <p>If a root cause is identified, the Problem Analyst updates the problem record with the details.</p>	Problem Analyst

Problem Investigation and Diagnosis process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.2.9	Update problem record with root cause	The Problem Analyst updates the problem record to indicate that a root cause has been found. The problem record is updated with any affected CIs.	Problem Analyst
SO 4.2.10	Workaround identified?	If a workaround is identified, the workflow moves to SO 4.2.11. If no workaround is identified, the workflow moves to SO 4.2.16.	Problem Analyst
SO 4.2.11	Verify workaround	The Problem Analyst creates a problem task and assigns it to the Investigation category in order to test the suitability of the identified workaround for resolving related incidents.	Problem Analyst
SO 4.2.12	Workaround successful?	If the workaround is successful, the workflow moves to SO 4.2.13. If the workaround is not successful, the workflow moves to SO 4.2.16.	Problem Analyst
SO 4.2.13	Update problem record with workaround	Update the workaround (in the known error and the problem) and inform stakeholders.	Problem Analyst
SO 4.2.14	Root cause or workaround determined?	The Problem Coordinator validates the results of the problem task. If the root cause is determined, the workflow moves to SO 4.2.15. If the root cause is not determined, the workflow moves to SO 4.2.16, and then determine whether additional resources are needed or whether escalation is required.	Problem Coordinator
SO 4.2.15	Update any related open Incidents	Review any related open incidents and advise the assigned Incident Analyst that a root cause and/or workaround has been identified. (An update will be made to the Activity Log in the incident record when the problem record is saved with an updated workaround).	Problem Coordinator
SO 4.2.16	Verify whether to continue investigation	The Problem Analyst determines whether to continue with the investigation, start problem resolution, or recommend abandonment.	Problem Analyst

Problem Investigation and Diagnosis process, continued

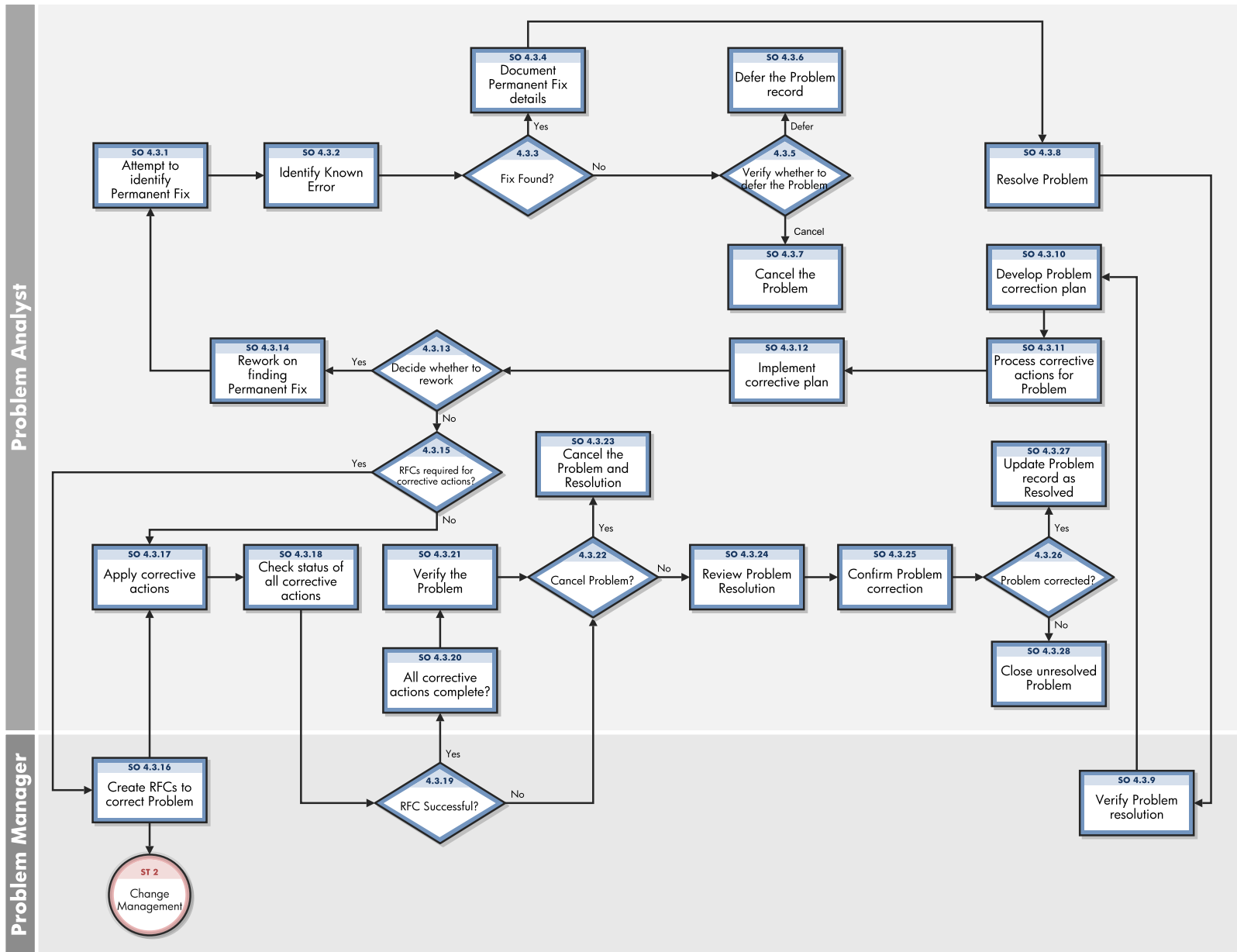
Process ID	Procedure or Decision	Description	Role
SO 4.2.17	Continue, defer, or abandon investigation?	<p>If the Problem Analyst decides to continue the investigation, the workflow moves to SO 4.2.6.</p> <p>If the Problem Analyst determines they do not have the capabilities to investigate and determine the root cause of the problem (that is, they do not have the skill level or the available time), the Problem Analyst documents the reason that a root cause is not found, the Problem Coordinator is informed, and the workflow moves to SO 4.2.18.</p> <p>If the problem can be abandoned, the workflow moves to SO 4.2.19.</p> <p>If the problem can be deferred, the workflow moves to SO 4.2.20.</p>	Problem Analyst
SO 4.2.18	Re-assign resources	The Problem Coordinator needs to re-assigns the problem to other resource to continue the problem investigation. The problem is moved back to Categorization phase with the Assign status again, and the workflow moves to SO 4.1.10.	Problem Coordinator
SO 4.2.19	Abandon the problem	The Problem Analyst abandons the problem ticket.	Problem Analyst
SO 4.2.20	Defer the problem investigation	<p>The Problem Analyst defers the problem investigation for a specific period of time. The reason for deferring the problem is detailed in the ticket. Periodically, the Problem Manager reviews the deferred problems to determine the appropriate action.</p> <p>Reasons for deferring problem include the following:</p> <ul style="list-style-type: none"> • The likelihood of recurrence is low • The cost of resolving the problem is very high • There is currently no plan to investigate the problem 	Problem Analyst

Problem Resolution (process SO 4.3)

After the Problem Management Investigation phase has identified the root cause of an incident, the Problem Resolution phase starts. In collaboration with specialist staff, the Problem Analyst assesses the means of resolving the problem. If necessary, the Problem Analyst requests for an RFC according to change management procedures, and links the RFC to the problem record.

The Problem Resolution phase comprises activities that identify and apply a solution to a problem.

The following figure illustrates the Problem Resolution workflow:



Problem Resolution process

Process ID	Procedure or Decision	Description	Role
SO 4.3.1	Attempt to identify permanent fix	<p>The Problem Analyst attempts to identify a permanent fix for the problem record. Workarounds may be found at this point, if they were not found in the previous phase. The workarounds are tested and documented, if successful.</p> <p>Sometimes, other teams or vendors are involved in identifying the fix for the problem. The problem ticket may incorporate many tasks that are assigned to various analysts or teams who are working towards the problem resolution.</p>	Problem Analyst
SO 4.3.2	Identify Known Error	If needed, mark the problem record as a known error for helpdesk's reference and to contribute to the known error knowledge base.	Problem Analyst
SO 4.3.3	Fix found?	<p>If a permanent fix is identified, it is documented.</p> <p>If a permanent fix is not identified, it is verified for closure or deferral.</p>	Problem Analyst
SO 4.3.4	Document permanent fix details	The Problem Analyst documents the permanent fix details in the problem record and updates the Knowledge Management Database with the permanent fix details. Then, the workflow moves to SO 4.3.8.	Problem Analyst
SO 4.3.5	Verify whether to defer the problem	<p>The Problem Analyst decides whether to defer or cancel the problem. If the problem is waiting for vendor resolution or for resource or budget approval, the problem is deferred, and the workflow moves to SO 4.3.6.</p> <p>If the problem is canceled, the workflow moves to SO 4.3.7.</p>	Problem Analyst
SO 4.3.6	Defer the problem record	The Problem Analyst defers the problem record for a period of time.	Problem Analyst
SO 4.3.7	Cancel the problem	The Problem Analyst closes the problem ticket and marks it as canceled.	Problem Analyst
SO 4.3.8	Resolve problem	In collaboration with specialist staff, the Problem Analyst assesses the means of resolving the problem. If necessary, they complete an RFC according to Change Management procedures, and link the RFC to the problem record.	Problem Analyst

Problem Resolution process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.3.9	Verify problem resolution	The Problem Manager reviews the history of the problem and its resolution, and then makes a final decision as to whether or not the problem is corrected. If the problem is corrected, the workflow moves to SO 4.3.10.	Problem Manager
SO 4.3.10	Develop problem correction plan	The Problem Analyst develops a plan that details all the corrective actions that must be performed to fix the problem. The Corrective Action Plan must include documenting the results of any monitoring that may have been implemented to monitor the problem resolution.	Problem Analyst
SO 4.3.11	Process corrective actions for problem	The Problem Analyst processes the problem record and prepares to implement the corrective actions. Problem tasks may be created and assigned to the Resolution category in order to execute the corrective actions.	Problem Analyst
SO 4.3.12	Implement corrective plan	The schedule to implement the fix is identified and updated in the correction plan. The correction plan is executed.	Problem Analyst
SO 4.3.13	Decide whether to rework	The Problem Analyst checks the implementation result and decides whether to rework the problem correction or abandon the problem fix.	Problem Analyst
SO 4.3.14	Rework on finding permanent fix	If the plan must be reworked, the Problem Analyst updates the problem status to Work In Progress. Then, the workflow moves to SO 4.3.1.	Problem Analyst
SO 4.3.15	RFCs required for corrective actions?	The Problem Analyst determines if any CIs must be modified in order to implement the resolution. If RFCs are required to resolve the problem, the Problem Manager is informed and the workflow moves to SO 4.3.16. If RFCs are not required to resolve the problem, the Problem Analyst can apply non-CI or pre-approved changes, and the workflow moves to SO 4.3.17.	Problem Analyst

Problem Resolution process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.3.16	Create RFCs to correct problem	The Problem Manager creates RFCs, links them to the problem, and inform Change Manager if required. The Problem Manager monitors the RFCs that are required to correct the problem.	Problem Manager
SO 4.3.17	Apply corrective actions	Some Problem resolutions require both non-CI-related activities and activities that affect CIs. The Problem Analyst applies non-CI corrective actions to fix the error.	Problem Analyst
SO 4.3.18	Check status of all corrective actions	The Problem Analyst checks the status of all the corrective actions that are applied to the problem record.	Problem Analyst
SO 4.3.19	RFC successful?	The Problem Manager checks the RFCs from the Change Management process to verify that they are successful. If the RFCs are successful, the status of all corrective actions are checked. If the RFCs are not successful, abandonment of the RFCs is recommended.	Problem Manager
SO 4.3.20	All corrective actions complete?	If all corrective actions are complete, the Problem Analyst begins to monitor the resolution.	Problem Analyst
SO 4.3.21	Verify the problem	The Problem Analyst verifies the resolution and the corrective actions to determine whether the problem can be abandoned or deferred.	Problem Analyst
SO 4.3.22	Cancel problem?	If the resolution to the problem needs to be canceled, the process moves to SO 4.3.23. If the resolution does not need to be canceled, the corrective action continues.	Problem Analyst
SO 4.3.23	Cancel the problem and resolution	The Problem Analyst closes the problem ticket and sets it to the "canceled" state.	Problem Analyst

Problem Resolution process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.3.24	Review problem resolution	The Problem Analyst reviews the history of the problem and its resolution, and then determines whether the problem is corrected.	Problem Analyst
SO 4.3.25	Confirm problem correction	The Problem Analyst reviews the problem history and resolution data, and then confirms that the affected personnel no longer experience the problem.	Problem Analyst
SO 4.3.26	Problem corrected?	If the problem is not corrected, the problem is set to the "unresolved" state and closed. Then, the workflow moves to SO 4.3.28. If the error is corrected, the workflow moves to SO 4.3.27.	Problem Analyst
SO 4.3.27	Update problem record as resolved	The Problem Analyst sets the problem record to the "resolved" state. The Problem Analyst closes the problem ticket, or sends it to Problem Manager for review and closure.	Problem Analyst
SO 4.3.28	Close unresolved problem	The Problem Analyst sets the problem record to the "unresolved" state and closes it. Sometimes, the problem record may be reworked. In such cases, the ticket is assigned to other teams, or the ticket's status is modified.	Problem Analyst

Problem Review and Closure (process SO 4.4)

After a problem has been resolved, it is automatically forwarded from the Problem Resolution phase to the Problem Review phase. In this phase, the problem(s) must be reviewed to determine and validate whether it has been resolved.

After a problem has been reviewed and closed, it is forwarded from the Problem Review phase to the Problem Closure phase. The problem record must be formally closed when any change has been completed and successfully reviewed, and the resolution has been applied.

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 the recurrence of incidents or mistakes.

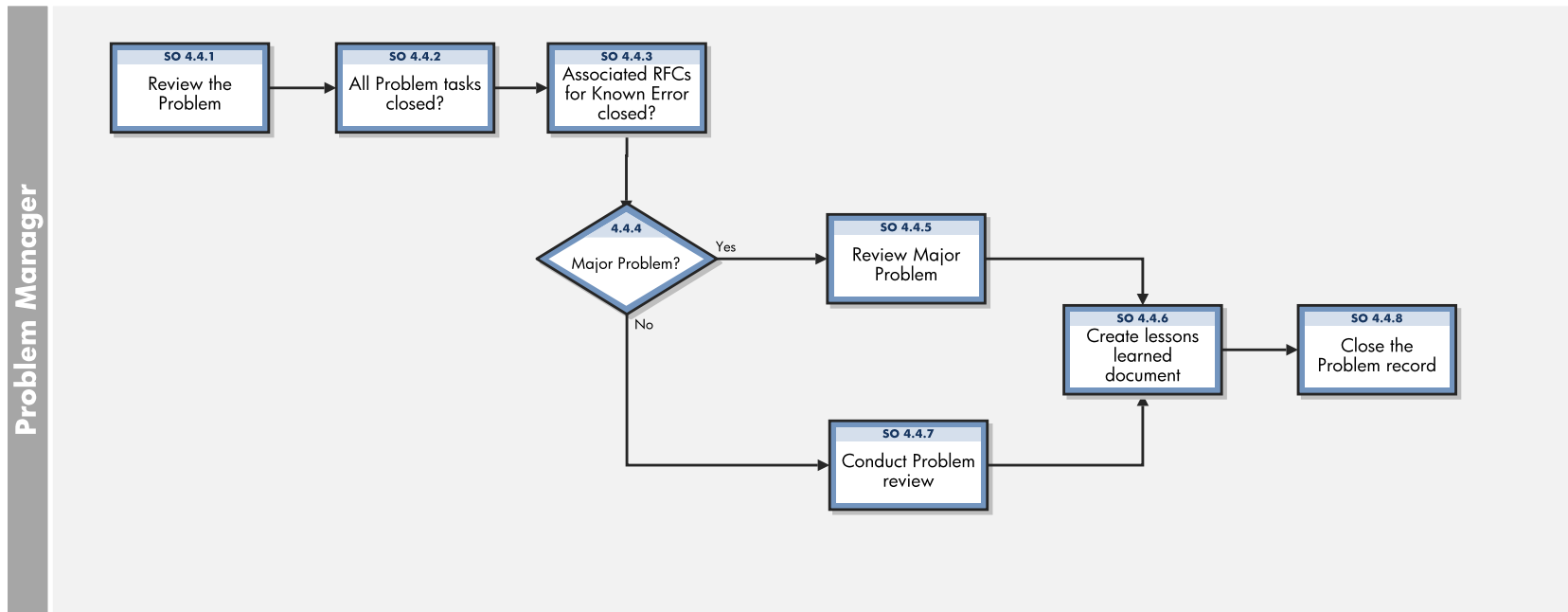
Problem reviews typically include the following elements:

- 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 and incidents)
- Recurring problems of a particular classification component or location
Deficiencies caused by lack of resources, training, or documentation
- Non-conformance (for example, against standards, policies, and legislation)
- Problems identified as known errors in planned releases
- Staff resource commitment in resolving incidents and problems
- Recurrence of resolved incidents or problems
- Improvements to the service or to the problem management process should be recorded and entered into a service improvement plan. This information should be added to the problem management knowledge base. All relevant documentation should be updated (for example, user guides and system documentation).

The following figure illustrates the Problem Review and Closure workflow:



Problem Review and Closure process

Process ID	Procedure or Decision	Description	Role
SO 4.4.1	Review the problem	The Problem Manager reviews the problem to determine whether it can be closed and to determine the reason for the closure.	Problem Manager
SO 4.4.2	All problem tasks closed?	The Problem Manager checks whether there any problem tasks are not closed. If there are open tasks, the task owner is requested to close or to cancel it.	Problem Manager
SO 4.4.3	Associated RFCs for known error closed?	The Problem Manager checks whether there any associated RFCs are not closed. If there are open RFCs, the RFC owner is requested to close or to cancel it.	Problem Manager
SO 4.4.4	Major problem?	If the problem is major, a formal major review is conducted. If the problem is not major, a regular review is conducted.	Problem Manager
SO 4.4.5	Review major problem	After every major problem (as determined by the organization's priority system), a review must be conducted to determine the lessons learned. Specifically, the review should examine the following items: <ul style="list-style-type: none"> • Actions correctly performed • Actions incorrectly performed • What can be done better in the future • How to prevent recurrence of the problem • Whether there has been any third-party responsibility • Whether any follow-up actions are needed. 	Problem Manager

Problem Review and Closure process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.4.6	Create lessons learned document	A “lessons learned” document is created and placed in SKMS, and all stakeholders are informed. The Problem Manager sends necessary details for service or process improvement to the Service Improvement Process, if required.	Problem Manager
SO 4.4.7	Conduct problem review	The Problem Manager initiates problem review activities and coordinates the formal review process. All parties involved in the problem resolution are included in the review, which summarizes what went well, what could be done better next time, what went wrong, and why some things went wrong.	Problem Manager
SO 4.4.8	Close the problem record	The Problem Manager closes the problem record by providing appropriate the closure code and comments.	Problem Manager

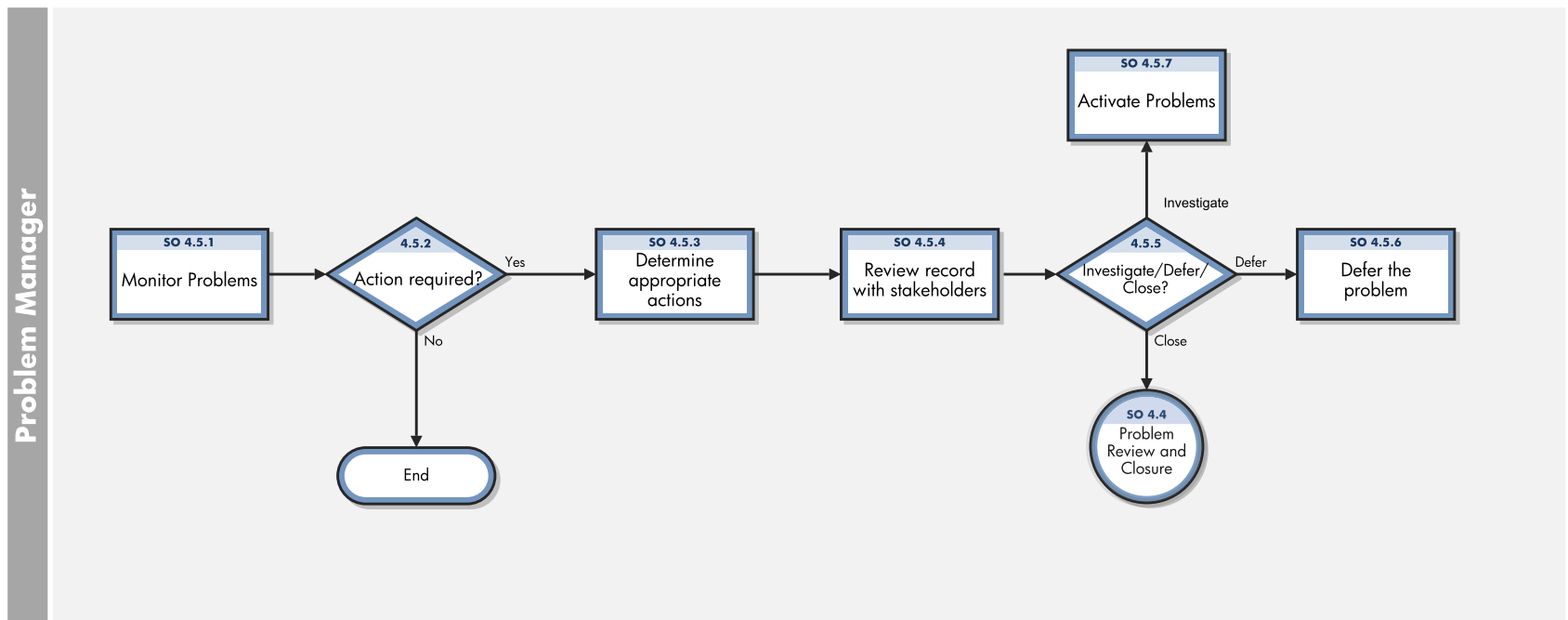
Problem Monitoring (process SO 4.5)

Problem management monitors the continuing impact of problems on user services. In the Problem Monitoring process, the Problem Manager periodically reviews the problem records and monitors the progress of activities in those records against the target dates that are agreed with stakeholders.

The Problem Manager evaluates the progress of those activities against the plans and associated budget. In the event that the impact of a problem becomes severe, the Problem Manager escalates the problem. In some cases, the Problem Manager may refer the escalated problem to an appropriate board to increase the priority of the request for change or to implement an urgent change.

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

The following figure illustrates the Problem Monitoring workflow:



Problem Monitoring process

Process ID	Procedure or Decision	Description	Role
SO 4.5.1	Monitor problems	<p>The Problem Manager reviews the Problem records periodically, and compiles a list or report of the problem records for review. This list or report includes the following items:</p> <ul style="list-style-type: none"> • Active problem records (to evaluate progress against the planned schedule and associated budget) • Deferred problem records (to evaluate whether they should remain in deferred status) <p>The review may also be triggered by new releases or by changes being implemented.</p> <p>The Problem Manager identifies the appropriate action for the records. Deferred records are activated or closed. Active records may be deferred or abandoned for various reasons.</p>	Problem Manager
SO 4.5.2	Action required?	<p>If any action is required, it is performed. If no action is required, the monitoring process continues.</p>	Problem Manager
SO 4.5.3	Determine appropriate actions	<p>The Problem Manager identifies the appropriate action for the record. Possible actions include the following:</p> <ul style="list-style-type: none"> • Record is closed as the problem is not relevant anymore • Record is investigated • Record is deferred 	Problem Manager
SO 4.5.4	Review record with stakeholders	<p>The actions for the records are reviewed with the stakeholders.</p>	Problem Manager
SO 4.5.5	Investigate/Defer/Close?	<p>Determine whether the problem is still relevant. If a deferred problem record needs to be worked on, it is activated.</p> <p>If the problem is not relevant, the problem record is checked for closure and deferring.</p>	Problem Manager

Problem Monitoring process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.5.6	Defer the problem	The problem record is deferred. The tentative activation date is entered in the problem record. If a problem must be deferred, the activation dates may need to be modified.	Problem Manager
SO 4.5.7	Activate problems	The Problem Manager updates a deferred problem record with scheduling and resource information. The manager also moves the problem record to the appropriate state for the resumption of work. The record is activated, coordinated by the Problem Coordinator, and worked upon by the assigned Problem Analyst.	Problem Manager

Chapter 13

Problem Management Details

HPService Manager uses the Problem Management application to enable the Problem Management process. The main function of Problem Management is to identify and resolve problems.

In Problem Management, the Problem Manager categorizes 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.

This section includes the following topics:

- ["Problem form after escalation from incident" below](#)
- ["Problem form details" on page 195](#)

Problem form after escalation from incident

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

The following screen-shot illustrates a new problem form:

Problem Details

Problem ID * PM10019	Assignment Group * Hardware
Phase * Problem Detection, Logging and Categorization	Problem Coordinator
Status * Open	Related Incident Count 1
Service * MyDevices	Category * problem
Primary CI adv-nam-desk-116	Area * performance
Affected CI Count 0	Subarea * performance degradation
SLA Target Date 03/18/10 16:12:57	Impact * 4 - User
Root Cause Target Date	Urgency * 2 - High
Solution Target Date	Priority 3 - Average
Resolution Target Date	
Title * Desktop reboots with BIOS message CPU temperature critical	
Description * Critical CPU temperature causes frequent reboots	
Root Cause Description	

After you save the new problem form, the problem moves to the Problem Categorization phase. The following screen-shot illustrates this change:

Problem - PM10014

Title: Desktop reboots with BIOS message CPU temperature critical

Description: Critical CPU temperature causes frequent reboots

Affected Service: MyDevices Problem ID: PM10014

Status: Categorize

Phase: Categorization Known Error:

Categorization

Category: problem Impact: 4 - User

Subcategory: performance Urgency: 2 - High

Area: performance degradation Priority: 3 - Average

Assignment Group: Assignee:

Workflow



Problem form details

The following table identifies and describes some of the features of problem forms:

Problem form details

Label	Description
Problem ID	Specifies the unique ID of the problem. This is a system-generated field.
Title	<p>A short description that summarizes the problem. This field is pre-populated with data from an incident when a user opens a problem from the incident.</p> <p>This is a required field.</p>
Description	<p>A detailed description of the problem. This field is pre-populated with data from an incident when a user creates a problem from the incident.</p> <p>This is a required field.</p>
Affected Service	<p>Specifies the service that is affected by the problem. This field is pre-populated with data from an incident when a user opens a problem from the incident.</p> <p>For more information about this field, see the "Affected service" section of the table in "Service Desk Interaction Management form details" on page 84.</p> <p>This is a required field.</p>
Phase	<p>This is a system-generated field.</p> <p>The following phases are available out-of-box:</p> <ul style="list-style-type: none">• Problem Detection, Logging, and Categorization• Problem Categorization• Problem Investigation• Problem Resolution• Problem Review• Problem Closure• Problem Abandonment

Problem form details, continued

Label	Description
Status	<p>Specifies the status of the problem. This field may affect the phase of the problem. All status changes must be performed manually. When the status changes, the problem phase may change automatically. There are several reasons to change the status of a problem (for example, when you are waiting for information from a vendor).</p> <p>The following statuses are available out-of-box:</p> <ul style="list-style-type: none"> • Open — The problem has been opened, but it is not currently being worked on. • Categorize — The problem is being categorized. • Assign — The problem is being assigned to the appropriate resource. • Work In Progress — The problem is being addressed. • Pending — The problem is pending for a period of time. The Problem Coordinator has contacted the vendor for information or for a part, or the Problem Coordinator has contacted the user for more information. • Deferred — Because of several possible constraints, the resolution of this problem must be postponed. • Resolved — A permanent fix is identified, and the problem is resolved. • Closed — The problem is closed or canceled. • Abandoned — The problem is abandoned (this only occurs in the Abandonment phase).
Known Error	<p>If set to true, it indicates that the problem is identified as a known error. A problem can be identified as a known error during any phase.</p>
Category	<p>This field is pre-populated with the default category. If a default category is not defined, you must select a category before open a new problem form.</p> <p>The out-of-box data is only “problem”. The problem category can be shared by Service Desk or Incident categories. You can also define new categories according to your needs.</p>
Subcategory	<p>The second level of categorization. This field is pre-populated with data from an escalated incident.</p> <p>Service Manager displays different lists of subcategories, depending on the category that you selected. The subcategories are defined on a category.</p>

Problem form details, continued

Label	Description
Area	<p>The third level of classification, mainly used for reporting purposes. This field is pre-populated with data from an escalated incident.</p> <p>Service Manager displays different lists of areas, depending on the category and subcategory that you selected. The areas are defined on a subcategory.</p>
Impact	<p>This field is pre-populated with data from an incident. It specifies the impact that the problem has on the business. The impact and the urgency are used to calculate the priority.</p> <p>The following impacts are available out-of-box:</p> <ul style="list-style-type: none"> • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User <p>The out-of-box data is the same as Interaction Management and Incident Management.</p>
Urgency	<p>This field is pre-populated 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 more information about this field, see "Service Desk Interaction Management form details" on page 84.</p>
Categorization > Priority	<p>The order in which to address this problem in relation to other problems. The priority value is calculated by using the initial impact and urgency. This field only appears when problems that are being updated or escalated from incidents.</p>

Problem form details, continued

Label	Description
Categorization > Assignment Group	<p>The group that is assigned to work on the problem. For more information about this field, see "Incident Management form details" on page 146.</p> <p>The out-of-box data consists of default assignment groups for use as examples of types of assignment groups.</p> <div data-bbox="477 499 1369 611" style="background-color: #f0f0f0; padding: 5px;"><p>Tip: You may want to change the sample assignment groups to meet your own needs.</p></div> <p>The following assignment groups are available out-of-box:</p> <ul style="list-style-type: none">• Application• Email / Webmail• Field Support• Hardware• Intranet / Internet Support• Network• Office Supplies• Office Support• Operating System Support• SAP Support• Service Desk• Incident Manager• Problem Coordinators• Problem Managers• Service Manager <p>This is a required field when status starts from Assign and phase starts from Categorization.</p>

Problem form details, continued

Label	Description
Categorization > Assignee	The name of the person who is assigned to work on this problem. If the Assignment Group field 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 that you select should be a member of the Assignment Group.
Workflow section	Displays a figure of the problem workflow. Also indicates the phase that the problem is currently in, and traces the phase transition history.
Affected Configuration Items section > 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 become 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 is the primary CI. Every CI that connects to the mail service (that is, that has Microsoft Outlook installed) is an affected CI.
Affected Configuration Items section > Affected CIs' table	The affected CIs are CIs that will have an issue when the primary CI has an issue. These fields must be filled in manually and are for information only. This data does not drive any action and is not required.
Affected Configuration Items section > Affected CI Count	A system-generated count of the number of CIs that are affected by the outage. The count does not include the primary CI. The affected CI count is based on the number of items entered in the Affected Configuration Items section. The affected CI count is calculated based on the Assessment section in the Affected CIs table.
Tasks section	<p>The user can add tasks during any phase of a problem. Every task must be finished before the problem can be closed. To add a new task, click the Tasks section, and then click the Link New Task button. Service Manager provides users with a quick view of some of the most important fields in the task in the Tasks section. The data displayed includes the following information:</p> <ul style="list-style-type: none"> • Task ID • Status • Phase • Priority • Title

Problem form details, continued

Label	Description
Related Records section > Link Type	Specifies a relationship type between the problem and the target ticket. The following groups of link types are available out-of-box: <ul style="list-style-type: none"> • Caused Interactions • Related Incidents • Caused Changes • Solved By Changes • Related Problems
Related Records section > Link Existing/New Record button	After you select a link type, use these two buttons to associate the problem with a target ticket, or to create a new target ticket and associate it with this problem.
Related Records section > All Related Records table	Displays information on all the records that are related to this problem. The data displayed includes the following information: <ul style="list-style-type: none"> • ID • (Relation) Type • Phase • Status • Title
Related Records section > Duplicate of Problem	Verifies whether this problem is a duplicate of another problem. If the problem is a duplicate, enter the duplicate problem ID in this field. Then, manually close the problem by clicking More > Close Duplicate Problem .
Related Records section > Duplicate Problems	Identifies problems that are duplicates of this problem. This field can be populated manually, or automatically, when other problems are verified as duplicates of this problem.

Problem form details, continued

Label	Description
Related Records section > Related Incident Count	This is a system-generated field. The related incident count is the number of incidents that are related to the problem, as recorded in the screlation table. To relate an incident to a problem, click the Related Records section, select Link Type as Related Records , and then click the Link Existing Record button.
Investigation and Resolution section > Expected Resolution Date	The expected problem resolution date should be approximately the same as the SLA Target date. The expected problem resolution date is the date when you plan to close the record. This should be done before the SLA Target date. This field has the Problem Management past due alert attached to it. This field appears when the problem enters Investigation phase. It becomes a required field in the “Work In Progress” and “Investigation” phases.
Investigation and Resolution section > Expected Root Cause Identified Date	Specifies the date by which the identification of the root cause of the problem is expected. You should base the date on the target date and on the identified dates in the SLA. This field appears in the “Investigation” phase to assist prioritization and planning in problem management processing. The field becomes a required field when the status changes to “Work In Progress” and the phase changes to “Investigation”.
Investigation and Resolution section > Solution Identified Date	The date when you identify the solution. This field appears when the problem enters the “Investigation” phase, and becomes required when the status changes to “Resolved”.
Investigation and Resolution > Root Cause	A detailed description of the cause of the problem. You cannot move on from the Problem Investigation phase until you have entered a description in this field. That phase is not complete until the cause of the problem is known.
Investigation and Resolution > Workaround	Describes a temporary solution or workaround.
Investigation and Resolution section > Estimated Man Days	Specifies a resource estimate to diagnose and resolve the problem. This data does not drive any action and is not required.

Problem form details, continued

Label	Description
Investigation and Resolution > Estimated Cost	Provides a resource (cost) estimate to diagnose and resolve the problem. This data does not drive any action and is not required.
Investigation and Resolution > Solution	Describes a permanent solution to the problem. This field is required when the problem status changes to "Resolved".
Closure Code	Uses a pre-defined closure code to specify the way in which the problem was closed. The out-of-box data is defined in the probcause table. This field is required when a problem is closed or abandoned. This field is populated in the closure wizard, and then automatically populated in the Summary section of the problem form.
Closure Comments	Comments to close the problem. This field is populated in the closure wizard, and then automatically populated in the Summary section of the problem form.