HP Service Manager

Software Version: 9.41

For the supported Windows® and UNIX® operating systems

Processes and Best Practices Guide (Codeless Mode)

Document Release Date: September 2015
Software Release Date: September 2015

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

For a complete list of open source and third party acknowledgements, visit the HP Software Support Online web site and search for the product manual called HP Service Manager Open Source and Third Party License Agreements.

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: https://softwaresupport.hp.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** 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 site at: https://softwaresupport.hp.com.

This website 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 website 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hp.com/web/softwaresupport/access-levels.

HPSW Solutions Catalog accesses the HPSW Integrations and Solutions Catalog portal website. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710.

Contents

Chapter 1: Introduction 11

Chapter 2: Service Desk Overview 12

Service Desk within the ITIL framework 13

Service Desk application 13

Service Desk process overview 14

Interaction categories 16

Interaction phases 17

Service Desk user roles 17

Input and output for Service Desk Interaction Management 18

Key performance indicators for Service Desk Interaction Management 19

ITIL 2011 Key Performance Indicators 19

COBIT 4.1 Key Performance Indicators 19

RACI matrix for Service Desk Interaction Management 20

Chapter 3: Service Desk Workflows 21

Self-Service by User (process SO 0.1) 22

Interaction Handling (process SO 0.2) 27

Interaction Escalation (process SO 0.3) 30

Close Interaction (process SO 0.4) 33

Cancel Interaction (process SO 0.5) 36

Chapter 4: Service Desk Details 38

New interaction form 39

Interaction form after escalation 40

Service Desk Interaction Management form details 42

Interaction categories 48

Escalate Interaction 51

Chapter 5: Incident Management Overview 53

Incident Management within the ITIL framework 53

Incident Management application 54

Notes for Incident Management implementation 54
Incident Closure process 54
Incident Management process overview 55
Incident Management categories 56
Incident Management phases 57
Incident Management tasks 58
Incident Task phases 58
Incident Management user roles 58
Input and output for Incident Management 60
Key performance indicators for Incident Management 60
ITIL 2011 Key Performance Indicators 61
COBIT 4.1 Key Performance Indicators 61
RACI matrix for Incident Management 63
Chapter 6: Incident Management Workflows 64
Incident Logging and Categorization (process SO 2.1) 65
Incident Assignment (process SO 2.2) 68
Incident Investigation and Diagnosis (process SO 2.3) 71
Incident Resolution and Recovery (process SO 2.4) 75
Incident Review and Closure (process SO 2.5) 78
Incident Escalation (process SO 2.6) 81
SLA Monitoring (process SO 2.7) 85
OLA and UC Monitoring (process SO 2.8) 88
Chapter 7: Incident Management Details 92
Incident form after escalation from Service Desk 92
Categorize incident form 93
Investigate incident form 94
Recover incident form 95
Review incident form 95
Incident Management form details 96
Chapter 8: Problem Management Overview 107
Problem Management within the ITIL framework 107
Differences between Problem Management and Incident Management 108

The Problem Management application 108

Problem Management workflows and categories 108

Problem tasks 109

Problem Management alerts 109

Problem management process overview 109

Problem management phases 112

Problem Management user roles 113

Input and output of Problem Management 114

Key Performance Indicators for Problem Management 116

ITIL 2011 Key Performance Indicators 117

COBIT 4.1 Key Performance Indicators 117

RACI matrix for Problem Management 118

Chapter 9: Problem Management Workflows 120

Problem Detection, Logging, and Categorization (process SO 4.1) 121

Problem Investigation and Diagnosis (process SO 4.2) 125

Problem Resolution (process SO 4.3) 130

Problem Review and Closure (process SO 4.4) 136

Problem and Known Error Monitoring (process SO 4.5) 140

Chapter 10: Problem Management Details 144

Problem form for problems opened from an incident 144

Problem form details 148

Chapter 11: Change Management Overview 155

Change Management within the ITIL framework 155

Change Management application 156

Differences between Change Management and Request Fulfillment 156

Change Management process overview 157

Change categories and phases 158

Change Management categories 159

Change Management phases 159

Change Management tasks 160

Change Task phases 160

Change Management user roles 162

Input and output for Change Management 164

Key performance indicators for Change Management 165

ITIL 2011 Key Performance Indicators 165
COBIT 4.1 Key Performance Indicators 166
RACI matrix for Change Management 167
Chapter 12: Change Management Workflows 170
Change Proposal (process ST 2.0) 171
Register RFC (process ST 2.1) 174
Standard Change (process ST 2.2) 177
Normal Change (process ST 2.3) 180
Emergency Change (process ST 2.4) 185
Review and Close Change (process ST 2.5) 189
Chapter 13: Change Management Details 193
Change Management form created from a problem 193
Change Management form details 195
Chapter 13: Knowledge Management Overview 203
Knowledge Management Within The ITIL Framework 203
Knowledge Management Application 204
Types of Knowledge Documents in Service Manager 204
Knowledge Management Categories 205
Knowledge Groups 205
Knowledge Management Profiles 205
Generic OOB Knowledge Management Document Phases 206
Knowledge Management Process Overview 208
Knowledge Management User Roles 208
Key Interfaces with Other Processes 210
Key performance indicators for Knowledge Management 211
RACI Matrix For Knowledge Management 212
Chapter 14: Knowledge Management Workflows 213
Contribute and Approve Knowledge Document (process ST 7.1) 214
Search, View and Utilize Knowledge Document (Process ST 7.2) 218
Maintain and Continually Improve Knowledge (Process ST 7.3) 221
Chapter 15: Knowledge Management Details 225

Knowledge Management Form - Contribute Knowledge 225
Knowledge Management Form - Search Knowledgebase (Advanced Search) 226

Chapter 16: Configuration Management Overview 229
Configuration Management within the ITIL framework 229
Configuration Management application 230
HP Universal Configuration Management Database 232
Baselines 232
Baseline section 233
Managed state 234
Managed State section 234
Actual state 234
Actual State section 235
CI relationships 235
CI Relationship section (CI visualization) 235
Configuration Management process overview 236
Configuration Management user roles 239
Input and output for Configuration Management 239
Key performance indicators for Configuration Management 240
ITIL V3 key performance indicators 241
COBIT 4.1 key performance indicators 241
RACI matrix for Configuration Management 242

Chapter 17: Configuration Management Workflows 243
Configuration Management Planning (process ST 3.1) 244
Configuration Identification (process ST 3.2) 250
Configuration Control (process ST 3.3) 255
Configuration Status Accounting and Reporting (process ST 3.4) 260
Configuration Verification and Audit (process ST 3.5) 266
Master data management (process ST 3.6) 271

Chapter 18: Configuration Management Details 277
MyDevices configuration item form 277
Configuration Management form details 278
Configuration Item types and subtypes 286
Managed State subsections 289

Chapter 19: Request Fulfillment Overview 291
Request Fulfillment within the ITIL framework 291
Request Fulfillment application 292
Differences between Request Fulfillment and Change Management 293
Key elements of Request Fulfillment 294
Request Model 294
Product Catalog 294
Vendors 295
Requests 295
Request Tasks 295
Orders 295
Authorization processing 295
Request Fulfillment process overview 296
Request Fulfillment user roles 298
Input and output for Request Fulfillment 300
Key performance indicators for Request Fulfillment 300
ITIL 2011 Critical Success Factors and Key Performance Indicators 301
RACI matrix for Request Fulfillment 303
Chapter 20: Request Fulfillment Workflows 304
Receive Request (process SO 3.1) 305
Request Logging (process SO 3.2) 308
Request Authorization (process SO 3.3) 309
Request Fulfillment (process SO 3.4) 310
Request Review (process SO 3.5) 314
Request Closure (process SO 3.6) 315
Chapter 21: Request Fulfillment Details 318
Request Fulfillment process flow 318
Request Fulfillment forms 320
Request Fulfillment form details 324
Request task forms 331
Request task form details 335
Chapter 22: Service Level Management Overview 341
Service Level Management within the ITIL Framework 341

Service Level Management Application 342

Input and output for Service Level Management 342

Key performance indicators for Service Level Management 344

ITIL recommended KPIs 344

Service Level Management Roles 345

RACI matrix for Service Level Management 347

Chapter 23: Service Level Management Workflows 348

Updating the Service Catalog (SD 2.1) 350

Create or Amend IT Services (SD 2.2) 351

SLRs and draft OLAs and UCs (SD 2.3) 353

Finalize SLRs/OLAs/UCs (SD 2.4) 356

Monitor Service Levels (SD 2.5) 357

Service Level Reporting (SD 2.6) 360

Perform Service Reviews (SD 2.7) 361

Service Improvement Plan (SD 2.8) 364

Review and Revise SLAs/OLAs/UCs (SD 2.9) 367

Chapter 24: Service Level Management Details 371

The Workflow for Agreements, Underpinning Contracts 372

Creating a new SLA, OLA or UC 374

The Draft phase 375

The Review phase 375

The Agreed phase 376

The Expired phase 378

Service Reviews and usages of SIPs/SQPs 378

Service Level Management forms 379

Service Level Management form details 383

Appendix A: Release and Deployment Management 389

Release and Deployment Management Overview 389

Release and Deployment Management within the ITIL framework 390

Release and Deployment Management application 391

Release and Deployment Management process overview 392

Release types 392

Release phases and transitions 392
Release tasks 393
Integration with Change Management 393
Release roles 393
Key performance indicators for Release and Deployment Management 394
Release and Deployment Management Workflow 395
Release Registration and Assess 395
Plan and Design 395
Build and Test 396
Training 396
Deployment 396
Back Out 396
Verification and Release Closure 396
Release and Deployment Management Details 397
Send Documentation Feedback 403

Chapter 1: Introduction

Welcome to the HP Service Manager Processes and Best Practices Guide (Codeless Mode). HP Service Manager enables organizations to manage their IT infrastructures efficiently and effectively. This guide documents the best practice Process Designer workflows that are standard with out-of-box Service Manager applications. It includes high-level workflow diagrams and step-by-step guidelines for the following Process Designer based modules: Change Management, Service Desk, Incident Management, Problem Management, Request Fulfillment, Knowledge Management, and Service Level Management.

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

This guide is intended for the customers of HP Service Manager 9.41 Codeless:

- New customers who have installed the out-of-box Service Manager 9.40 (server, client, and applications), and then upgraded to HP Service Manager 9.41 Codeless(server, client, and applications).

- Existing Process Designer Content Pack 4 customers who have upgraded server, client, and applications to HP Service Manager 9.41 Codeless

Other customers must read the *HP Service Manager Processes and Best Practices Guide (Classic Version)* instead of this document.

Chapter 2: Service Desk Overview

Note: The topics in this section are based on the Streamlined Interaction solution, which is introduced as of Service Manager 9.41. The Streamlined Interaction feature is optional and is disabled by default. You need to manually enable it before you read the topics in this section. To enable the Streamlined Interaction solution, see Service Manager 9.41 Help Center.

For information about the previous Service Desk application (Codeless mode) that is not based on the new Streamlined Interaction solution, see the *Service Manager 9.40 Processes and Best Practices Guide (Codeless Mode)*.

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" on the next page
- "Service Desk application" on the next page
- "Service Desk process overview" on page 14
- "Input and output for Service Desk Interaction Management" on page 18
- "Key performance indicators for Service Desk Interaction Management" on page 19
- "RACI matrix for Service Desk Interaction Management" on page 20

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. Service desk staff execute the incident management and request fulfillment processes 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 2011 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 when first contacted or whenever possible
- 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:

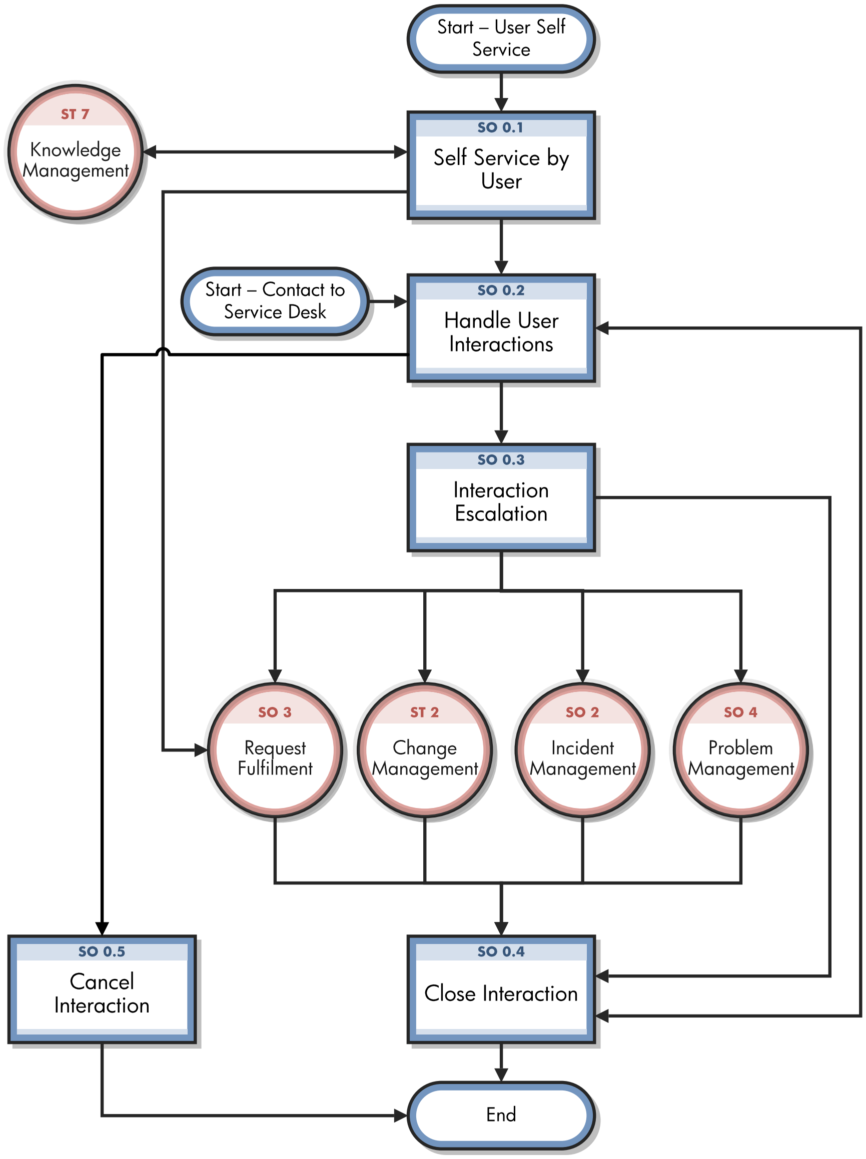
- Direct interactions between a user and the service desk by phone or by email
- User activities that occur from use of the self-service web portal (for example, searching the knowledge base, checking for status updates, or logging an interaction).

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 resolving any new complaints or compliments within the agreed upon time limits and then closed, or triggering fulfillment processes for the other types of interactions. The information gathered during the customer interaction can be used to open an incident, service request, or other fulfillment records. It can also be added to a record in another Service Manager application such as Incident 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), complaints, or compliments 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 (such as complaints and compliments) and to escalate others into fulfillment processes (such as Incident Management) requiring further action.

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 user request is a complaint or compliment, the Service Desk manager can handle the interaction and close it.
- If the user request can be resolved by the Service Desk agent on first contact, the Service Desk agent will use the interaction to trigger an incident or a service request, and then close the incident

or service request directly with the solution provided. Then, the interaction will be closed automatically.

- If the user request cannot be resolved without escalation, the Service Desk agent can register a new record in a fulfillment process (such as the incident, service request, problem, or change fulfillment process) based on the Service Desk interaction. Service Desk copies information from the interaction record into the newly created fulfillment record.

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 interaction is automatically closed accordingly.
- 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 send out survey based on the closed interaction. If the user still cannot print, the Service Desk agent may register a new interaction and then escalate the interaction to a new incident.
- If the user wishes to report a related or new issue, the Service Desk agent opens a new interaction detailing the new issue that the user needs to report.

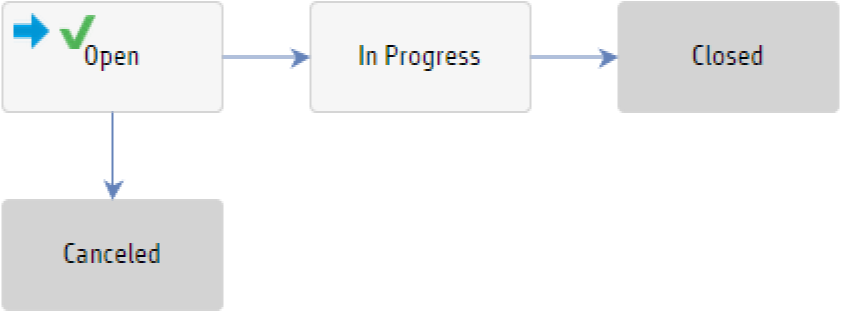
Interaction categories

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 complete an interaction. The phase also determines the forms that users see, and the actions that users can trigger manually.

The following figure shows the workflow phases for an interaction (complaint or compliment).



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	• Report all IT-related requests to the service desk or use the self-service web pages. • Validate solutions and answers provided by the IT department to a registered service request.
Service Desk Agent	• Register interactions based on contact with users. • Solve and close interactions. • Provide status updates to users on request. • Register incidents based on user interactions and assign them to the correct support groups. • Register requests for change, based on user interactions. • Register service requests, based on user interactions. • Register problems, based on user interactions. • Validate solutions provided by support groups.

User Interaction Management user roles, continued

Role	Responsibilities
	• Report and verify solutions to users. • Monitor Service Level Agreement (SLA) targets of all interactions. • Communicate about service outages to all users.
Service Desk Manager	• Appoint people to the required roles. • Manage resources assigned to the service desk. • Manage service desk activities. • Attend CAB meetings. • Report any issue that could significantly impact the business to senior managers. • Take overall responsibility for incident and service request handling on the service desk. • Monitor and report on service desk performance. • Make improvements to the service desk.

Input and output for Service Desk Interaction Management

Interactions can be triggered and resolved in several ways. The following table outlines the input and output 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
A user can contact Service Desk and give input by using instant messages, phone, email, self-service web pages, or other means.	Service Desk personnel can handle an interaction in the following ways: • If the interaction is a user complaint or compliment, the interaction is handled by Service Desk. • If the interaction can be resolved by Service Desk when first contacted, the interaction will be triggered to either an incident or a service request and closed by Service Desk directly with a solution provided.

Input and output for Service Desk Interaction Management, continued

Input to Service Desk Interaction Management	Output from Service Desk Interaction Management
	• If the interaction requires an incident, service request, problem, or change, the interaction is sent to different fulfillment processes.

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
First line fix	Percentage of records 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 2011 and COBIT 4.1 KPIs are included below.

ITIL 2011 Key Performance Indicators

The following are ITIL 2011 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 desk 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 for 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/I	A/R
SO 0.3	Interaction Escalation	R	R	A
SO 0.4	Close Interaction	R/I	R	A
SO 0.5	Cancel Interaction	R/I	R	A

Chapter 3: Service Desk Workflows

Note: The topics in this section are based on the Streamlined Interaction solution, which is introduced as of Service Manager 9.41. The Streamlined Interaction feature is optional and is disabled by default. You need to manually enable it before you read the topics in this section. To enable the Streamlined Interaction solution, see Service Manager 9.41 Help Center.

For information about the previous Service Desk application (Codeless mode) that is not based on the new Streamlined Interaction solution, see the *Service Manager 9.40 Processes and Best Practices Guide (Codeless Mode)*.

Every time a user contacts the service desk, as an interaction is logged. 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), complaints, or compliments reported by users who communicate with the service desk by using instant messages, phone, email, or self-service web pages.

The process enables Service Desk agents to easily log and resolve simple user requests and to escalate others into fulfillment processes 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 27
- "Interaction Escalation (process SO 0.3)" on page 30
- "Close Interaction (process SO 0.4)" on page 33
- "Cancel Interaction (process SO 0.5)" on page 36

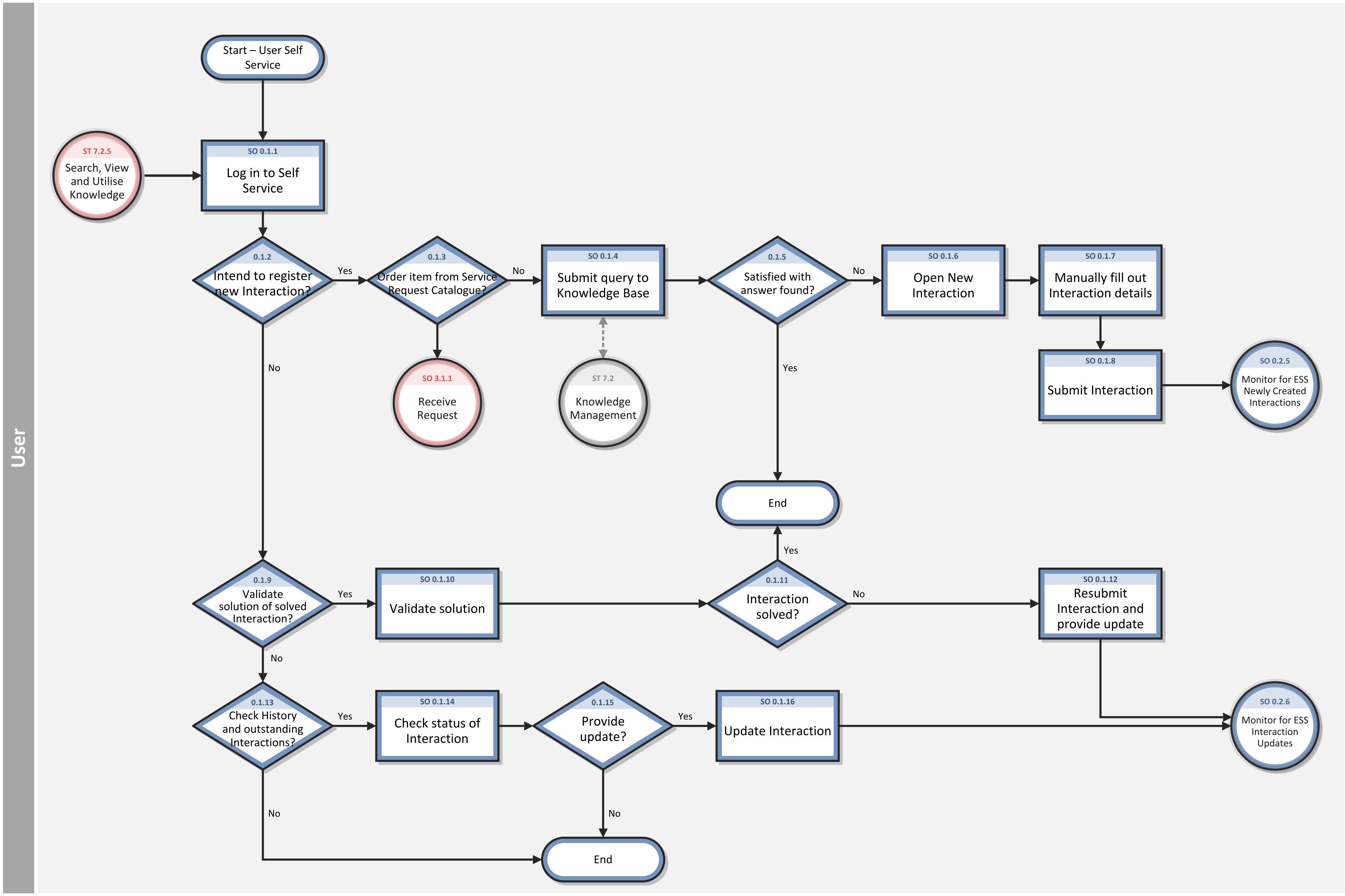
Self-Service by User (process SO 0.1)

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:


User
Start – User Self Service
ST 7.2.5
Search, View and Utilise Knowledge
SO 0.1.1
Log in to Self Service
0.1.2
Intend to register new Interaction?
Yes
0.1.3
Order item from Service Request Catalogue?
No
SO 0.1.4
Submit query to Knowledge Base
0.1.5
Satisfied with answer found?
No
SO 0.1.6
Open New Interaction
SO 0.1.7
Manually fill out Interaction details
SO 3.1.1
Receive Request
ST 7.2
Knowledge Management
Yes
SO 0.1.8
Submit Interaction
SO 0.2.5
Monitor for ESS Newly Created Interactions
No
End
Yes
0.1.9
Validate solution of solved Interaction?
Yes
SO 0.1.10
Validate solution
0.1.11
Interaction solved?
No
SO 0.1.12
Resubmit Interaction and provide update
No
0.1.13
Check History and outstanding Interactions?
Yes
SO 0.1.14
Check status of Interaction
0.1.15
Provide update?
Yes
SO 0.1.16
Update Interaction
SO 0.2.6
Monitor for ESS Interaction Updates
No
No
End

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	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
SO 0.1.9	Validate solution of	To validate the solution to a previously reported interaction, go to SO 0.1.10. If no, go to SO 0.1.13.	User

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

Process ID	Procedure or Decision	Description	Role
	solved interaction?		
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
SO 0.1.16	Update Interaction	There are two scenarios in which you may update an interaction and then require a Save button to save the updated information. • The Save button appears when a self-service user selects the option View Open Requests, selects an interaction, and clicks the Update button. Once the information is updated, the self-service user clicks **Save & Exit** to save the updated information in the request.	User

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

Process ID	Procedure or Decision	Description	Role
		• 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. Once you have added more information to the request or performed the changes, you can click **Save & Exit**.	

Interaction Handling (process SO 0.2)

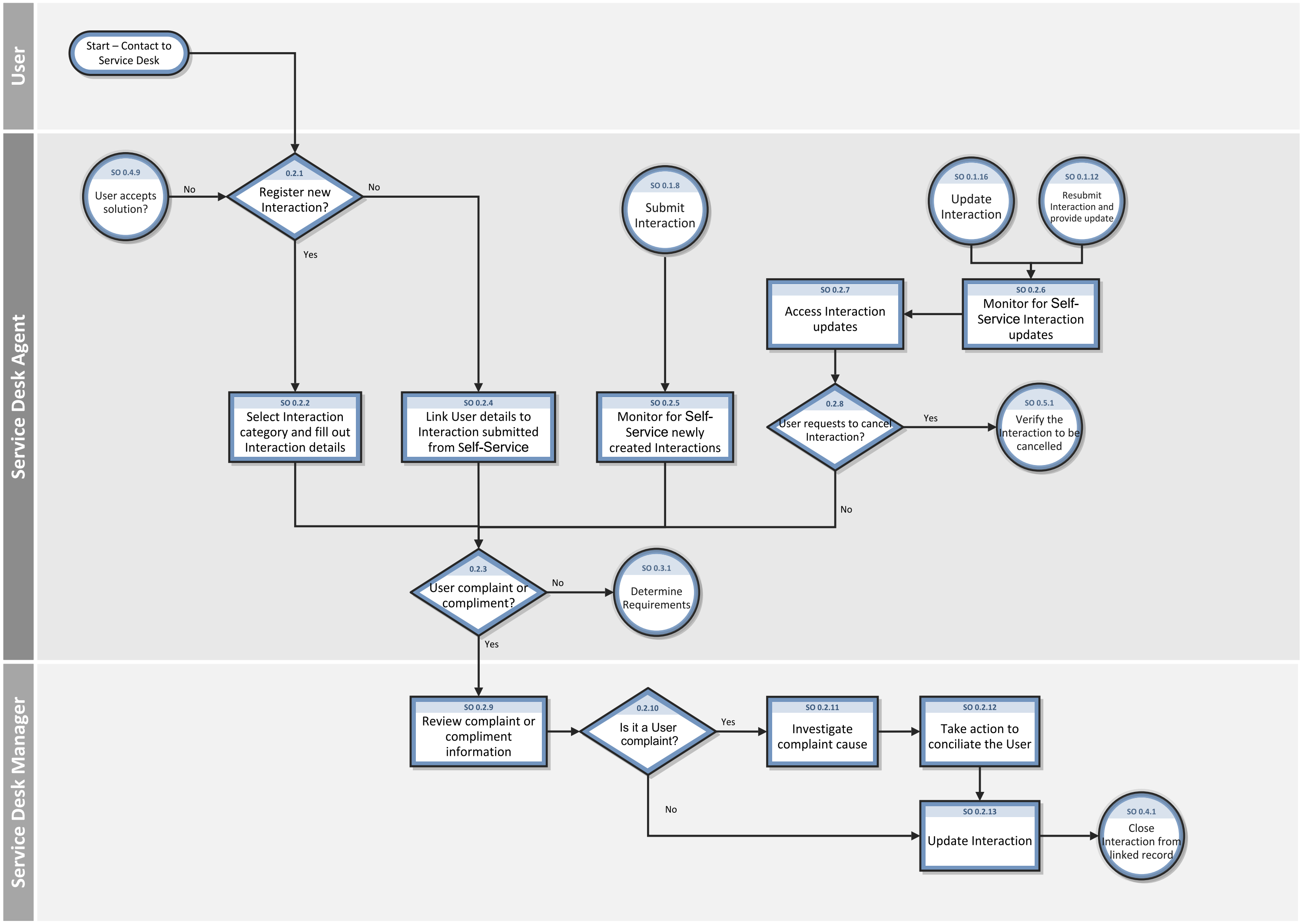
The service desk is responsible for handling all user interactions received by the self-service Web portal, email, or phone. The service desk attempts to resolve an interaction of user complaints or compliments.

Handling user complaints or compliments is the process that the Service Desk Manager is responsible for.

When the Service Desk Manager receives assigned interactions, the manager investigates the cause of the complaint or compliment 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 interaction with the agreed details, and then closes the interaction.

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:


User
Service Desk Agent
Service Desk Manager
Start – Contact to Service Desk
SO 0.4.9
User accepts solution?
No
0.2.1
Register new Interaction?
No
Yes
SO 0.1.8
Submit Interaction
SO 0.1.16
Update Interaction
SO 0.1.12
Resubmit Interaction and provide update
SO 0.2.7
Access Interaction updates
SO 0.2.6
Monitor for Self-Service Interaction updates
SO 0.2.2
Select Interaction category and fill out Interaction details
SO 0.2.4
Link User details to Interaction submitted from Self-Service
SO 0.2.5
Monitor for Self-Service newly created Interactions
0.2.8
User requests to cancel Interaction?
Yes
SO 0.5.1
Verify the Interaction to be cancelled
No
0.2.3
User complaint or compliment?
No
SO 0.3.1
Determine Requirements
Yes
SO 0.2.9
Review complaint or compliment information
0.2.10
Is it a User complaint?
Yes
SO 0.2.11
Investigate complaint cause
SO 0.2.12
Take action to conciliate the User
No
SO 0.2.13
Update Interaction
SO 0.4.1
Close Interaction from linked record

Interaction Handling (SO 0.2) process

Process ID	Procedure or Decision	Description	Role
SO 0.2.1	Register new Interaction?	If a new interaction is required, go to SO 0.2.2. If not, go to SO 0.2.4.	Service Desk Agent
SO 0.2.2	Select Interaction category and fill out Interaction details	Select the appropriate Interaction category from the available category list and fill out the required Interaction details such as a full Description, Contact, Service Recipient, and so on.	Service Desk Agent
SO 0.2.3	User complaint or compliment?	If the Interaction is a user complaint or compliment, go to SO 0.2.9. If not, go to SO 0.3.1 to determine what requirement of the user request is.	Service Desk Agent
SO 0.2.4	Link User details to Interaction submitted from Self-Service	In Self-Service Interaction, fill in the name of the caller in the Contact field and the name of the User in the Service Recipient field (if different).	Service Desk Agent
SO 0.2.5	Monitor for Self-Service newly created Interactions	If there are new Interactions, follow the same Interaction registration process.	Service Desk Agent
SO 0.2.6	Monitor for Self-Service Interaction updates	If Interactions are updated, they must be reassessed.	Service Desk Agent
SO 0.2.7	Assess Interaction updates	Evaluate Interactions that have been updated or resubmitted.	Service Desk Agent
SO 0.2.8	User requests to cancel Interaction?	If the User requests to cancel Interaction, go to SO 0.5.1 to verify the Interaction to be cancelled. If not, go to SO 0.2.3.	Service Desk Agent
SO	Review complaint or	The Service Desk Manager reviews the detailed information.	Service

Interaction Handling (SO 0.2) process, continued

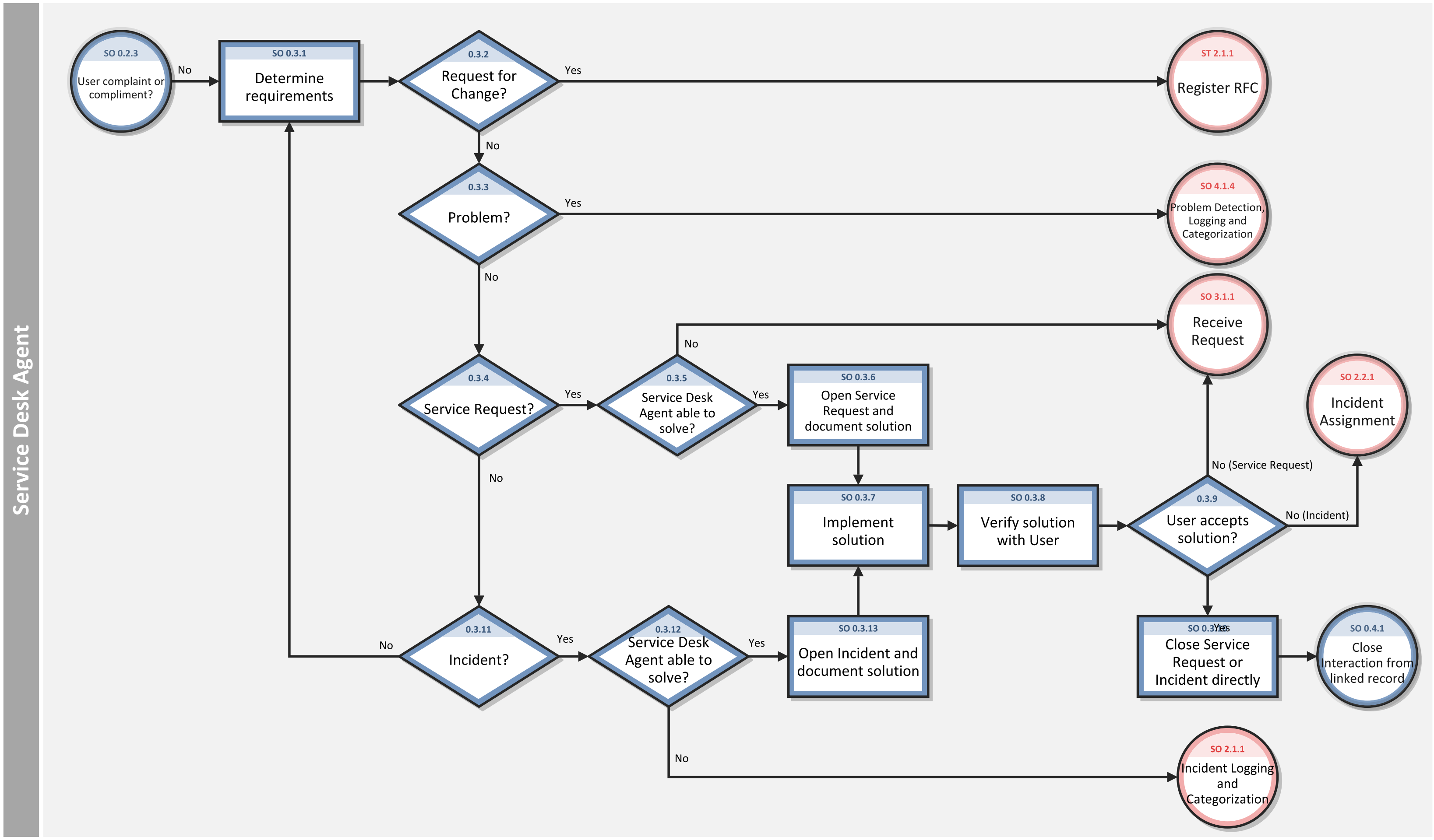
Process ID	Procedure or Decision	Description	Role
0.2.9	compliment information		Desk Manager
SO 0.2.10	Is it a User complaint?	If it is a user complaint, go to SO 0.2.11. If not, go to SO 0.2.13.	Service Desk Manager
SO 0.2.11	Investigate complaint cause	The Service Desk Manager investigates the cause 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 0.2.12	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 0.2.13	Update Interaction	The Service Desk Manager updates the Interaction with the agreed solution, and then go to SO 0.4.1 to close the Interaction.	Service Desk Manager

Interaction Escalation (process SO 0.3)

When an Interaction is received, the Service Desk Agent first determines if the Interaction is a service request, a request for change, a problem or an incident, and if so, logs the request.

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

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



Interaction 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 requirement of the user request is.	Service Desk Agent
SO 0.3.2	Request for Change?	If a Change is required, go to ST 2.1.1 to log the RFC. If not, go to SO 0.3.3.	Service Desk Agent
SO 0.3.3	Problem?	If a Problem is needed, go to SO 4.1.4 to create a new Problem. If not, go to SO 0.3.4.	Service Desk Agent
SO 0.3.4	Service Request?	If a Service Request is required, go to SO 0.3.5. If not, go to SO 0.3.11.	Service Desk Agent
SO 0.3.5	Service Desk Agent able to solve?	If the Service Desk Agent is able to solve the Service Request, go to SO 0.3.6. If not, go to Request Fulfillment process SO 3.1.1.	Service Desk Agent
SO 0.3.6	Open Service Request and document solution	The Service Desk Agent creates a new Service Request and documents the solution to be implemented.	Service Desk Agent
SO 0.3.7	Implement solution	The Service Desk Agent then implements the solution for the User.	Service Desk Agent
SO 0.3.8	Verify solution with User	The Service Desk Agent contacts the User and communicates the solution. The user should verify the solution and confirm that the Service Request is fulfilled or the Incident is resolved.	Service Desk Agent
SO	User accepts solution?	If the User accepts the solution, go to SO 0.3.10. If not, go to Request Fulfillment process SO 3.1.1	Service

Interaction Escalation (SO 0.3) process, continued

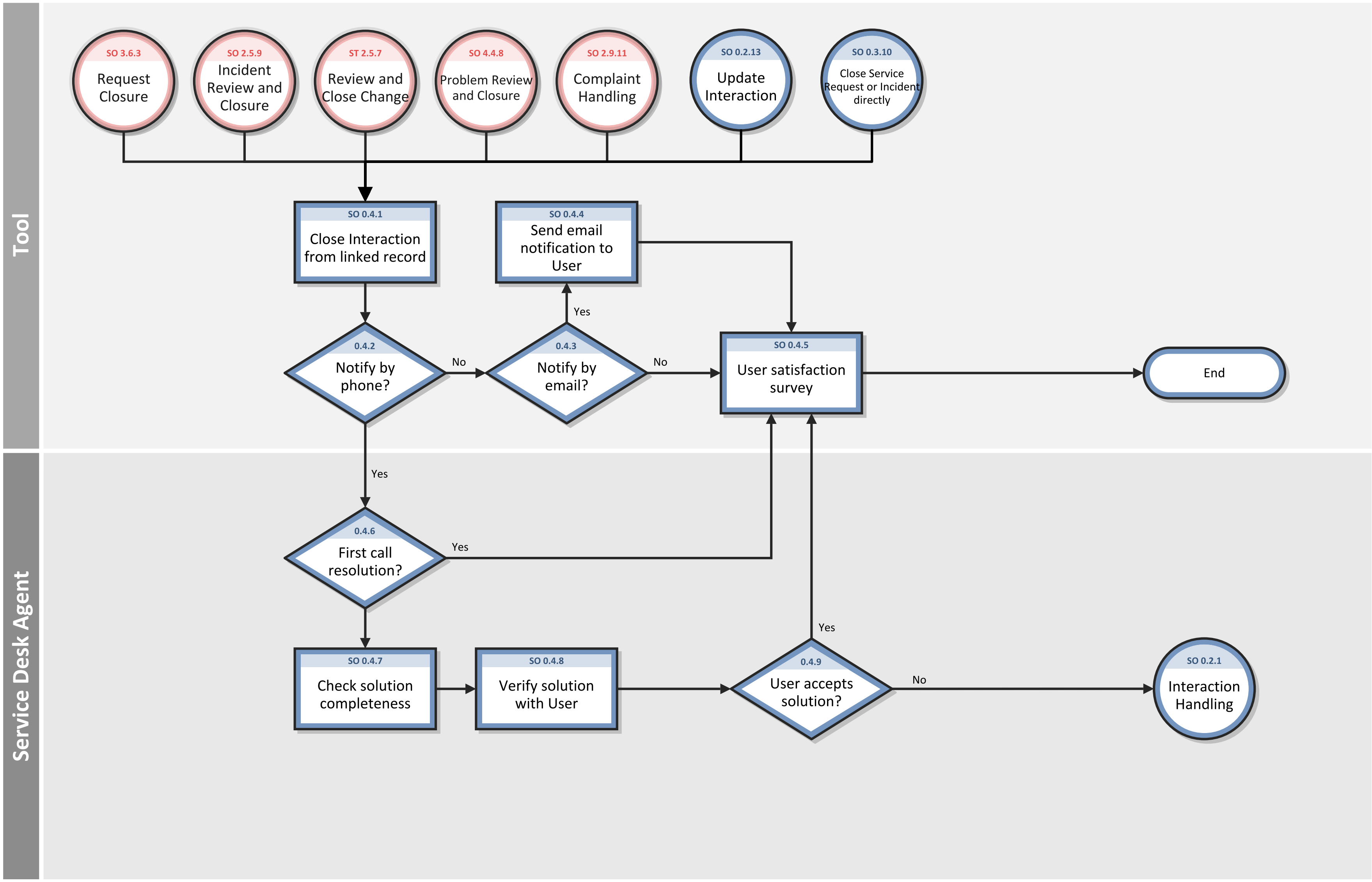
Process ID	Procedure or Decision	Description	Role
0.3.9		for Service Request or Incident Management process SO 2.2.1 for Incident assignment.	Desk Agent
SO 0.3.10	Close Service Request or Incident directly	The Service Desk Agent closes the Service Request or Incident on first intake.	Service Desk Agent
SO 0.3.11	Incident?	If it is an Incident, go to SO 0.3.12. If not, go to SO 0.3.1.	Service Desk Agent
SO 0.3.12	Service Desk Agent able to solve?	If the Service Desk Agent is able to solve the Incident, go to SO 0.3.13. If not, go to Incident Management process SO 2.1.1.	Service Desk Agent
SO 0.3.13	Open Incident and document solution	The Service Desk Agent creates a new Incident and documents the solution to be implemented. Then go to SO 0.3.7.	Service Desk Agent

Close Interaction (process SO 0.4)

When an interaction is solved by a related incident, change, request, or problem 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.

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


Tool
Service Desk Agent
SO 3.6.3
Request Closure
SO 2.5.9
Incident Review and Closure
ST 2.5.7
Review and Close Change
SO 4.4.8
Problem Review and Closure
SO 2.9.11
Complaint Handling
SO 0.2.13
Update Interaction
SO 0.3.10
Close Service Request or Incident directly
SO 0.4.1
Close Interaction from linked record
SO 0.4.4
Send email notification to User
0.4.2
Notify by phone?
No
0.4.3
Notify by email?
Yes
No
SO 0.4.5
User satisfaction survey
End
Yes
0.4.6
First call resolution?
Yes
SO 0.4.7
Check solution completeness
SO 0.4.8
Verify solution with User
0.4.9
User accepts solution?
Yes
No
SO 0.2.1
Interaction Handling

Interaction Closure (SO 0.4) process

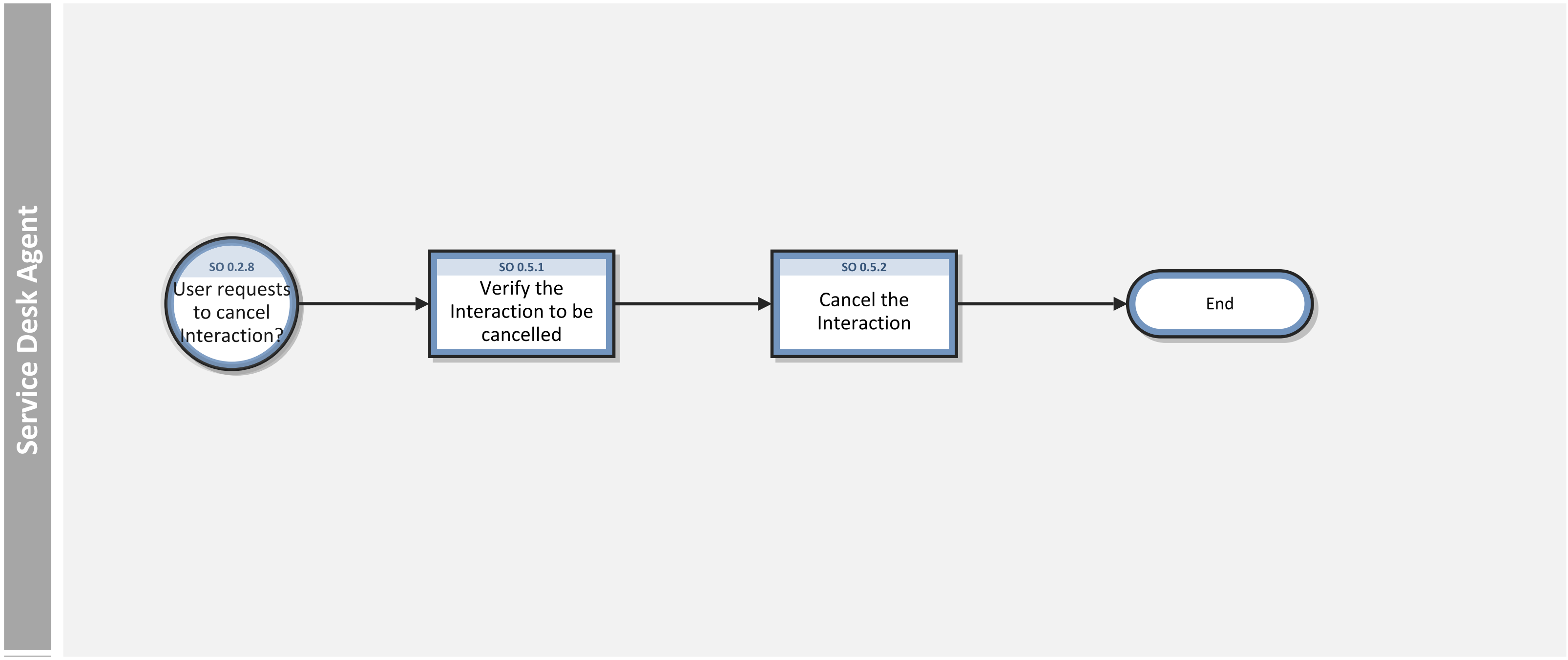
Process ID	Procedure or Decision	Description	Role
SO 0.4.1	Close Interaction from linked record	The Interaction closure is caused by the closure of an Incident, Change, Problem or Service Request, or the submission of a User complaint or compliment.	Tool
SO 0.4.2	Notify by phone?	If the Notify By method states that the User wants to be notified by phone, go to SO 0.4.6. If not, go to SO 0.4.3.	Tool
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, go to SO 0.4.5.	Tool
SO 0.4.4	Send email notification to User	Email notification is sent to User.	Tool
SO 0.4.5	User satisfaction survey	A user satisfaction survey that is automatically generated by the system can be sent out.	Tool
SO 0.4.6	First call resolution?	If the related Service Request or Incident is closed by Service Desk Agent on first contact, go to SO 0.4.5. If not, go to SO 0.4.7.	Service Desk Agent
SO 0.4.7	Check solution completeness	The Service Desk Agent checks the solution provided by fulfillment team.	Service Desk Agent
SO 0.4.8	Verify solution with User	The Service Desk Agent contacts the User and communicates the solution. The user should verify the solution and confirm that the incident is solved, the question or complaint is answered, or the Service Request is fulfilled.	Service Desk Agent
SO 0.4.9	User accepts solution?	If the User accepts the solution, go to SO 0.4.5. If not, go to SO 0.2.1 to register new Interaction.	Service Desk Agent

Cancel Interaction (process SO 0.5)

The Cancel Interaction process identifies the steps to cancel an interaction.

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

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


Service Desk Agent
SO 0.2.8
User requests to cancel Interaction?
SO 0.5.1
Verify the Interaction to be cancelled
SO 0.5.2
Cancel the Interaction
End

Cancel Interaction (SO 0.5) process

Process ID	Procedure or Decision	Description	Role
SO 0.5.1	Verify the Interaction to be cancelled	The Service Desk Agent verifies the User updates to check whether the Interaction can be cancelled or not.	Service Desk Agent
SO 0.5.2	Cancel the Interaction	The Service Desk Agent cancels the Interaction based on User updates.	Service Desk Agent

Chapter 4: Service Desk Details

Note: The topics in this section are based on the Streamlined Interaction solution, which is introduced as of Service Manager 9.41. The Streamlined Interaction feature is optional and is disabled by default. You need to manually enable it before you read the topics in this section. To enable the Streamlined Interaction solution, see Service Manager 9.41 Help Center.

For information about the previous Service Desk application (Codeless mode) that is not based on the new Streamlined Interaction solution, see the *Service Manager 9.40 Processes and Best Practices Guide (Codeless Mode)*.

HP Service Manager uses its Service Desk application to enable the Service Desk Interaction Management process. The main function of Service Desk is to monitor, track, and record calls and toopen fulfillment records, 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 a fulfillment process.

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

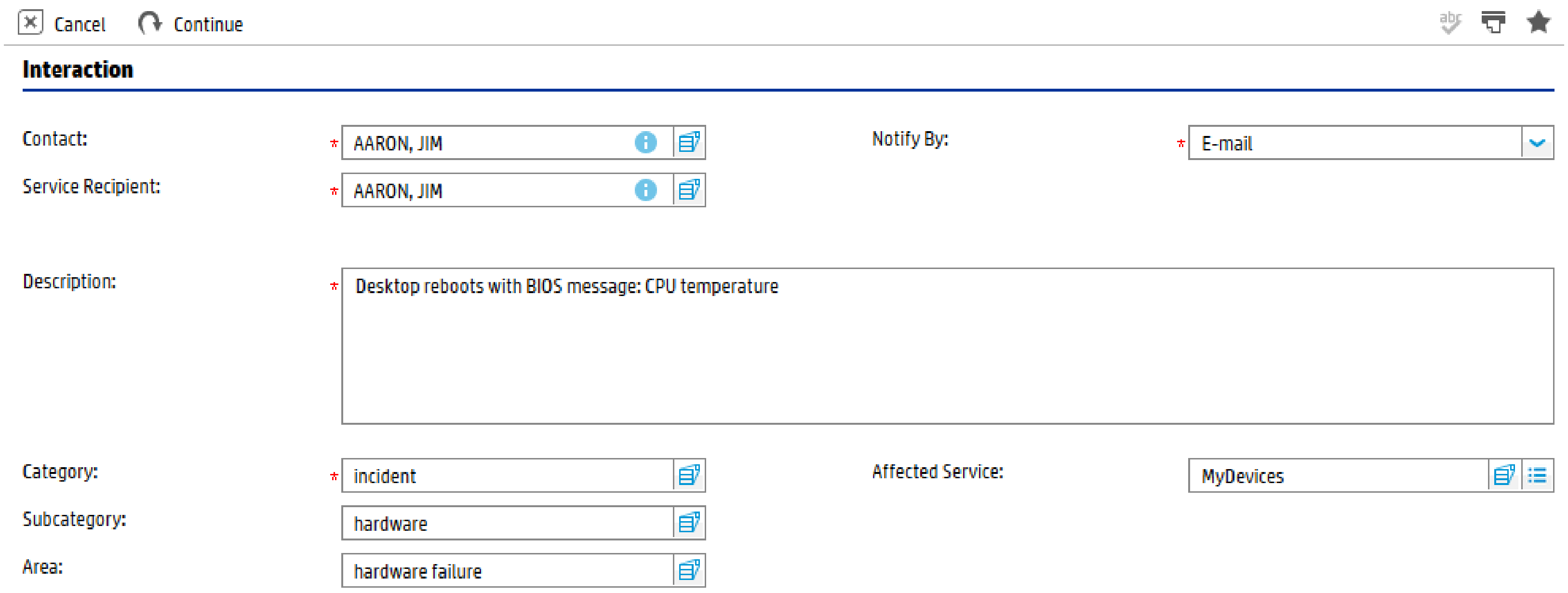
Topics in this section include:

- "New interaction form" on the next page
- "Interaction form after escalation" on page 40
- "Service Desk Interaction Management form details" on page 42
- "Interaction categories" on page 48

New interaction form

When a Service Desk Agent clicks **Create Streamlined 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 from that has been completed is illustrated in the following screenshot:



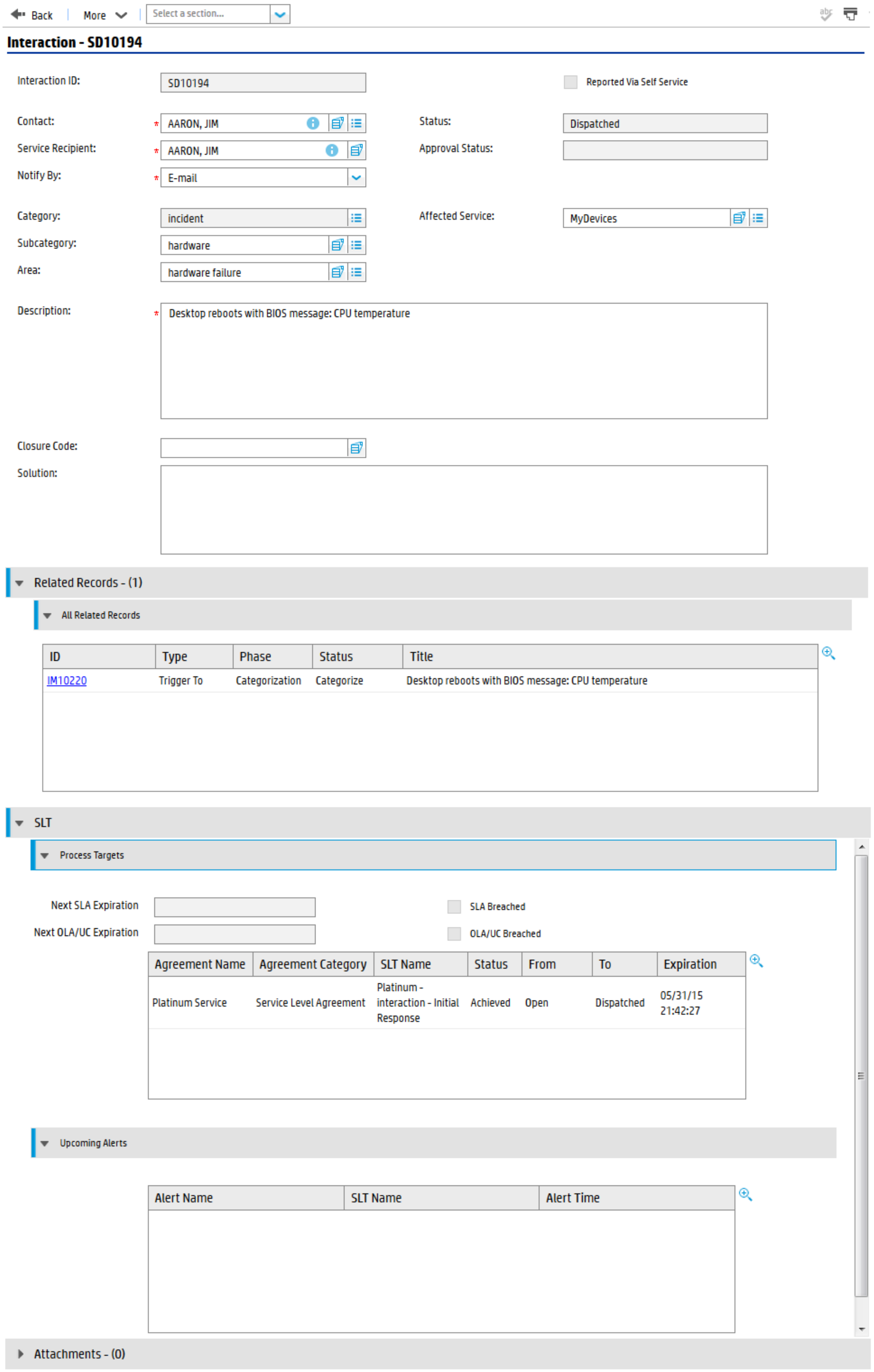
Interaction

Contact:	* AARON, JIM	Notify By:	* E-mail
Service Recipient:	* AARON, JIM		
Description:	* Desktop reboots with BIOS message: CPU temperature		
Category:	* incident	Affected Service:	MyDevices
Subcategory:	hardware		
Area:	hardware failure		

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:



Interaction - SD10194

Interaction ID: SD10194

□ Reported Via Self Service

Contact: * AARON, JIM

Status: Dispatched

Service Recipient: * AARON, JIM

Approval Status:

Notify By: * E-mail

Category: incident

Affected Service: MyDevices

Subcategory: hardware

Area: hardware failure

Description: * Desktop reboots with BIOS message: CPU temperature

Closure Code:

Solution:

Related Records - (1)

All Related Records

ID	Type	Phase	Status	Title
IM10220	Trigger To	Categorization	Categorize	Desktop reboots with BIOS message: CPU temperature

SLT

Process Targets

Next SLA Expiration

□ SLA Breached

Next OLA/UC Expiration

□ OLA/UC Breached

Agreement Name	Agreement Category	SLT Name	Status	From	To	Expiration
Platinum Service	Service Level Agreement	Platinum - interaction - Initial Response	Achieved	Open	Dispatched	05/31/15 21:42:27

Upcoming Alerts

Alert Name	SLT Name	Alert Time

Attachments - (0)

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.
Status	The options in this field have been revised to align with our new best practices. **Tip:** You may want to tailor these options to match your business needs. These statuses are available out-of-box: • Open — The interaction has been initially logged. For example, when the Service Desk Agent is still on the phone with the customer. • 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, problem, or request. • Pending Customer - The interaction is pending for User input to proceed its fulfillment process. • Pending Approval - The service catalog request is pending for approval. • Closed — The interaction is closed by the help desk or automatically after the related record is closed. • Canceled — The interaction is canceled by Service Desk Agent based on the user updates. • Resolved — The interaction is resolved when the linked incident is move to the "Resolved" status.
Contact	The Service Desk Agent populates this field with the person from whom the call was received. 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 includes a hover-over form that displays full name, telephone, and email address for the contact, if available.

Service Desk Interaction Management form details, continued

Label	Description
	This is a required field.
Service Recipient	The person who has the problem and needs it resolved. It is not necessarily the person who is calling to report the problem. Filling in this field automatically fills in the contact name from the contact record of who should be notified of the resolution. The Service Desk Agent populates this field with the person this issue is registered for. This field includes a hover-over form that displays full name, telephone, and email address if available for the service recipient. This is a required field.
Notify By	To notify the customer when the issue has been resolved, Service Manager prepopulates this field as E-mail. The user or the Service Desk Agent can change it to None or Telephone, if applicable. When the related fulfillment record is closed: • Selecting E-mail closes the interaction and sends an email to the contact • Selecting None closes the interaction without notifying the contact • Selecting Telephone tells the Service Desk Agent to ask the contact whether the solution is satisfactory. If the solution works for the customer, the Service Desk Agent closes the interaction. If it does not work, then the Service Desk Agent must open a new interaction. This is a required field.
Affected Service	The Service Desk Agent populates this field with the business service affected by the registered issue. Only business services the service recipient has a subscription for can be selected. ITIL 2011 is centered around services, so a service construct should always be defined for best practices. If you have not yet created a service construct, start with a catch-all service, such as My Devices. **Note:** The out-of-box options in this field are based on past Service Manager implementations. You should tailor these options to match your business needs. These business services are available out-of-box: • Applications • Email/Webmail • Handheld PDA & Telephony • Intranet • Internet

Service Desk Interaction Management form details, continued

Label	Description
	• My Devices (The My Devices service represents all personal devices that the user would use.) • Printing Selecting the service: • Validates that it is a valid service. An end user is more likely to know that the email service does not work than what part of the email service does not work. This is a required field.
Description	The Service Desk Agent populates this field with a detailed description of the interaction. When the location and telephone number differ from the contact details, the Service Desk Agent can record the correct information in the description field. **Note:** Service Manager searches this field when you perform an advanced or expert text search. This is a required field.
Closure Code	This field contains a predefined closure code, describing the way this issue has been solved. The out-of-box options in this field are based on Service Manager customer reference data. **Note:** You may want to tailor these options to match your business needs. These closure codes are available out-of-box: • Automatically Closed • Cancelled • Denied Service Catalog Request • Fulfilled • Invalid • Not Reproducible • Out of Scope • Request Rejected • Solved by Change/Service Request

Service Desk Interaction Management form details, continued

Label	Description
	• Solved by User Instruction • Solved by Workaround • Unable to solve • Withdrawn by User
Solution	This field contains a description of the solution used for this interaction. **Note:** Service Manager searches this field when you perform an advanced or expert text search.
Category	This field describes the type of interaction. The interaction type determines the process to escalate to when the interaction is not a user complaint or compliment. The categories are based on ITIL service-centric processes, and therefore focus on enabling assignment, reporting, and operational analysis for knowledge management purposes. From the category list: • Incident > Continue — You can relate the interaction to a new incident. • Request for Change > Continue — Service Manager creates a new change request. • Service Request/Request for Administration/Request for Information > Continue - You can relate the interaction to a new service request. • Problem > Continue - Service Manager creates a new problem. • Support Catalog > Continue - Support Catalog opens, allowing you to place an order. After an order is submitted, the interaction is given the category configured in the ordered support catalog item and a related record is created as defined in the ordered support catalog item as well. • Service Catalog > Continue — 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. • Complaint/Compliment > Continue - No related record is created. Service Desk handles such types of interactions. **Note:** The Service Desk Agent needs to have proper permissions to open corresponding fulfillment records.

Service Desk Interaction Management form details, continued

Label	Description
	For more information on categories and the subcategories and areas associated with them, see "Interaction categories" on page 48. This is a required field.
Subcategory	The Service Desk Agent populates this field with the subcategory of concern. 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 48.
Area	The third level of classifying an interaction, mainly used for reporting purposes. 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 48.
Assignment Group	The group assigned to work on the user complaint or compliment. For a description of this field see the Assignment Group field description in the Incident Management form details section as this field functions similarly. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. You may want to change the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail • Field Support • Hardware • Incident Managers • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • Problem Coordinators • Problem Managers • SAP Support

Service Desk Interaction Management form details, continued

Label	Description
	• Service Desk • Service Desk Analysts • Service Manager
Assignee	The name of the person assigned to work on the user complaint or compliment. 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.
Approval Status	This field is only used when you request something from the catalog. When you submit an order from the catalog, Service Manager automatically creates an interaction which, based on approval requirements, may have to be approved before it can be fulfilled. Service Manager populates this field with the current approval status for this interaction. These approval statuses are available out-of-box: • pending — The request has not been approved or a prior approval or denial has been retracted. • approved — All approval requirements are approved, or no approval necessary. • denied — The request has been denied.
Activities	The Activities section records information that Service Desk enters during the lifecycle of a user complaint or compliment. Every time you update a user complaint or compliment, 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. Self-Service updates from users are also displayed here.
Related Records	The Related Records section contains a list of all related records for the interaction. These may include related incidents, problems, changes, and requests.
SLT	The SLT (Service Level Target) section displays SLAs related to the interaction. SLAs in interactions are customer-related and selected, based on the customer contact or department and service related to the issue. The Process Targets define 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. **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.

Service Desk Interaction Management form details, continued

Label	Description
Continue button	The Service Desk Agent clicks this button to create an incident, problem, request, or change from this interaction. 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.
Cancel Interaction button	The Service Desk Agent clicks this button to cancel the interaction on behalf of the user.
Close button	The Service Desk clicks this button to close the user complaint or compliment. The customer's issue was resolved and requires no further action.
Fulfill button	The Service Desk handles the user complaint or compliment.
More > Send Survey	After interaction is closed, the Service Desk Agent can carry out a user satisfaction survey.

Interaction categories

The category hierarchy was designed to support the ITIL 2011 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, we recommend that you 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

Categories, subcategories, and areas, continued

Category	Subcategory	Area
complaint	service delivery	functionality
complaint	service delivery	performance
complaint	support	incident resolution quality
complaint	support	incident resolution time
complaint	support	person
compliment	service delivery	availability
compliment	service delivery	functionality
compliment	service delivery	performance
compliment	support	incident resolution quality
compliment	support	incident resolution time
compliment	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

Categories, subcategories, and areas, continued

Category	Subcategory	Area
incident	performance	system or application hangs
incident	security	security breach
incident	security	security event/message
incident	security	virus alert
problem	access	authorization error
problem	access	login failure
problem	data	data or file corrupted
problem	data	data or file incorrect
problem	data	data or file missing
problem	data	storage limit exceeded
problem	facilities	hardware failure
problem	facilities	miscellaneous
problem	facilities	supplies
problem	failure	error message
problem	failure	function or feature not working
problem	failure	job failed
problem	failure	system down
problem	hardware	hardware failure
problem	hardware	missing or stolen
problem	performance	performance degradation
problem	performance	system or application hangs
problem	security	security breach
problem	security	security event/message
problem	security	virus alert
request for administration	grant access	grant access
request for administration	other	other
request for administration	password reset	password reset

Categories, subcategories, and areas, continued

Category	Subcategory	Area
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
service request	Employee Off-boarding	
service request	Employee On-boarding	
service request	Hardware	
service request	Request for Administration	
service request	Request for Information	
service request	Software	
support catalog	support catalog	support catalog

Escalate Interaction

Depending on your selection, the **Continue** button opens different fulfillment records as follows:

- Escalate Interaction - Incident

  You can escalate Interactions in the following category to Incident:

  - incident

- Escalate Interaction - RFC

  You can escalate Interactions in the following category to RFC:

  - request for change

  Option 1: If change is open on Category in settings, when escalating an interaction to an RFC, a list of change categories is displayed from which the category for the new change request can be selected.

Option 2: If change is open on Change Model in settings, when escalating an interaction to an RFC, a list of Change Models is displayed from which the Change Model for the new change request can be selected.

- Escalate Interaction - Request

  You can escalate Interactions in the following categories to Request:

  - service request
  - request for information
  - request for administration

  Option 1: If request is open on Category in settings, when escalating an interaction to a request, a list of request categories is displayed from which the category for the new request can be selected.

  Option 2: If request is open on Request Model in settings, when escalating an interaction to a request, a list of Request Models is displayed from which the Request Model for the new request can be selected.

- Escalate Interaction - Problem

  You can escalate Interactions in the problem category to Problem.

Chapter 5: Incident Management Overview

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

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

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

Topics in this section include:

- "Incident Management within the ITIL framework" below
- "Incident Management application" on the next page
- "Incident Management process overview" on page 55
- "Input and output for Incident Management" on page 60
- "Key performance indicators for Incident Management" on page 60
- "RACI matrix for Incident Management" on page 63

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.

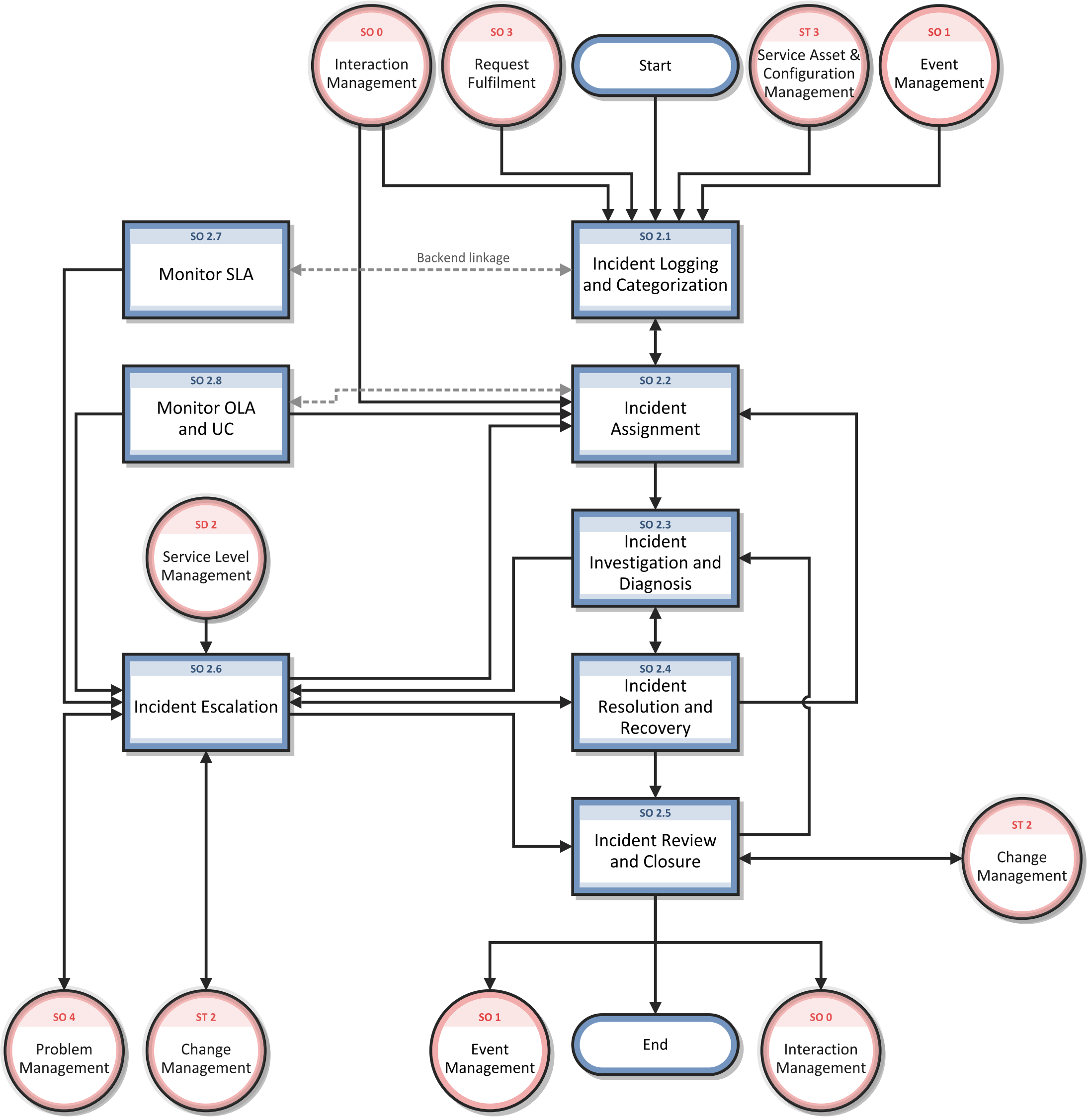
Legacy Service Manager customers who did not activate Service Desk and used a two-step incident close will find that this is no longer necessary, because the Service Desk application is now included.

Incident 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".



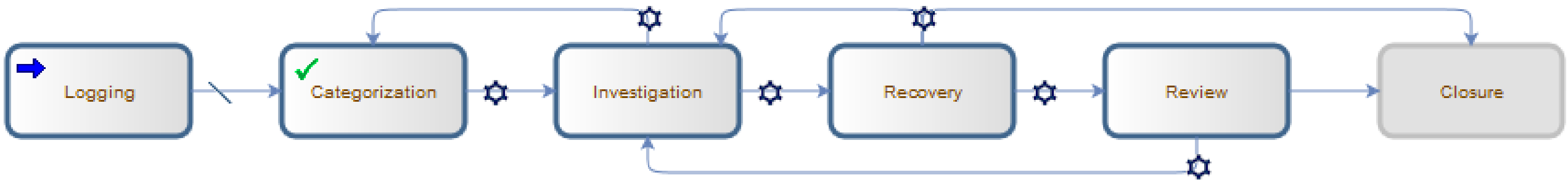
Incident Management categories

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.

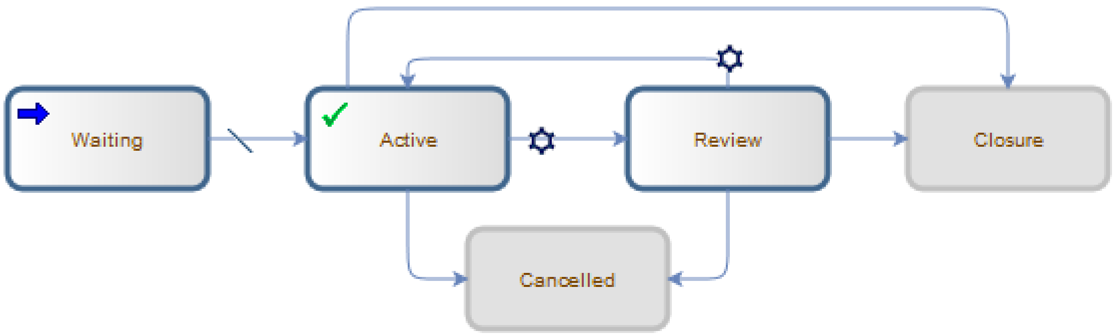
Incident Management tasks include:

- 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.
Service Desk Agent	• Register interactions based on contact with user. • Match user interaction to incidents, problems, known errors, or knowledge document. • Solve and close interactions. • Provide status updates to users on request. • Register incident based on a user interaction and assign to the correct support group. • Register Request for Change, based on a user interaction. • Register Service Request, based on a user interaction. • Validate a solution provided by a support group. • Report and verify a solution to a user. • Monitor Service Level Agreement (SLA) targets of all incidents registered and escalate, if required. • Communicate about service outages to all users.
Incident Analyst	• 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	• 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	• 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
• Customer interactions with the Service Desk, which can be triggered to incidents • Event management tool, which automatically opens incidents • Support staff	• Resolved incidents • Documented workarounds, solutions, or knowledge articles • New problems, changes, or incidents Incidents can also trigger several other Service Manager processes, as described in the next section.

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.
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 2011 and COBIT 4.1 KPIs are included below.

ITIL 2011 Key Performance Indicators

The following are ITIL 2011 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 6: Incident Management Workflows

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

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

- "Incident Logging and Categorization (process SO 2.1)" on the next page
- "Incident Assignment (process SO 2.2)" on page 68
- "Incident Investigation and Diagnosis (process SO 2.3)" on page 71
- "Incident Resolution and Recovery (process SO 2.4)" on page 75
- "Incident Review and Closure (process SO 2.5)" on page 78
- "Incident Escalation (process SO 2.6)" on page 81
- "SLA Monitoring (process SO 2.7)" on page 85
- "OLA and UC Monitoring (process SO 2.8)" on page 88

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.

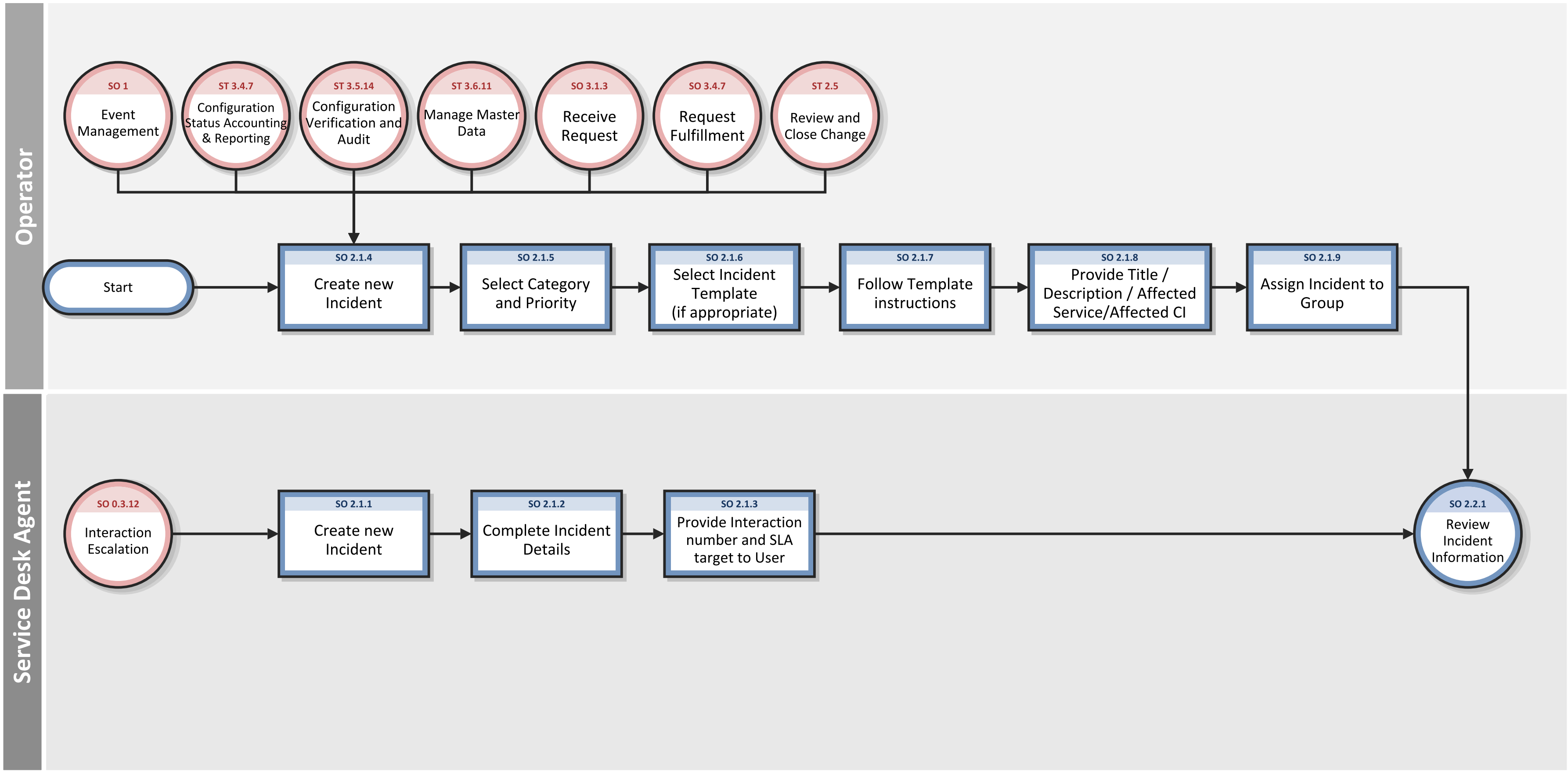
- If the incident is logged by the Service Desk Agent, most incident details are already provided by the interaction record. The Service Desk Agent verifies the Assignment Group to make sure the selected group is the most suitable group to solve the incident.
- If an incident is logged by an Operator,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

The 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	Complete Incident 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 2.1.3	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 2.1.4	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. If a new service request is identified as an incident or an incident occurs related to fulfillment activities, the Operator creates an incident from a service request. Go to SO 2.1.10 to select an Incident template (if appropriate).	Operator
SO 2.1.5	Select Category and Priority	Select the suitable Category and Priority by selecting the applicable impact level and urgency.	Operator
SO 2.1.6	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 2.1.7	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 2.1.8	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

Incident Logging and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
SO 2.1.9	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

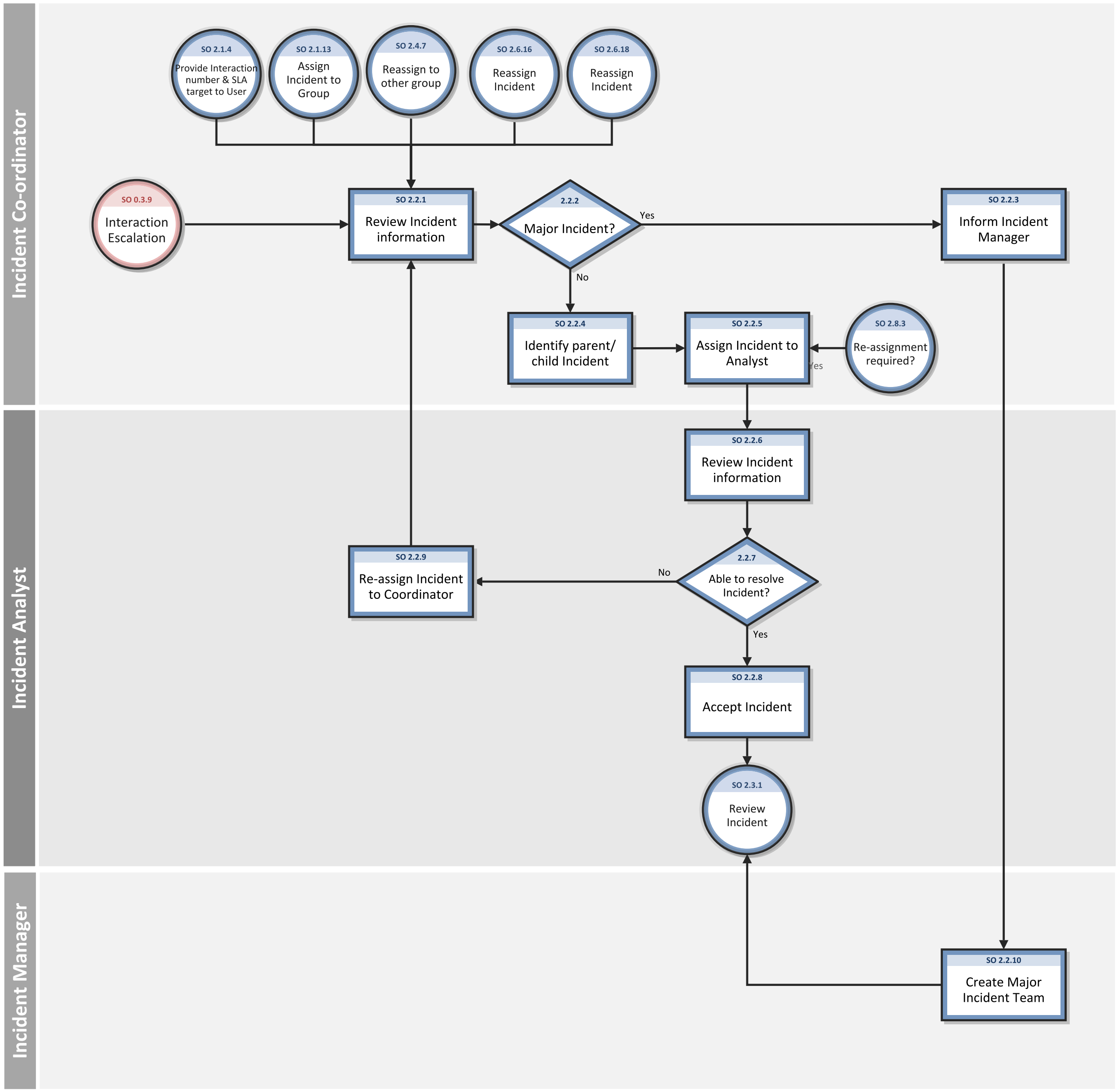
Incident Assignment (process SO 2.2)

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.

The Incident Assignment workflow is illustrated in the following figure:


Incident Co-ordinator
Incident Analyst
Incident Manager
SO 2.1.4
Provide Interaction number & SLA target to User
SO 2.1.13
Assign Incident to Group
SO 2.4.7
Reassign to other group
SO 2.6.16
Reassign Incident
SO 2.6.18
Reassign Incident
SO 0.3.9
Interaction Escalation
SO 2.2.1
Review Incident information
2.2.2
Major Incident?
Yes
No
SO 2.2.3
Inform Incident Manager
SO 2.2.4
Identify parent/ child Incident
SO 2.2.5
Assign Incident to Analyst
Yes
SO 2.8.3
Re-assignment required?
SO 2.2.6
Review Incident information
SO 2.2.9
Re-assign Incident to Coordinator
No
2.2.7
Able to resolve Incident?
Yes
SO 2.2.8
Accept Incident
SO 2.3.1
Review Incident
SO 2.2.10
Create Major Incident Team

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	Identify parent/child Incident	The operator identifies whether there is a need to create a parent-child record relationship to link multiple similar incidents together.	Operator
SO 2.2.5	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 2.2.6	Review Incident information	The Incident Analyst monitors the queue of incidents assigned to him/her and reviews the incoming incidents.	Incident Analyst
SO 2.2.7	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	Accept	The Incident Analyst accepts the incident.	Incident

Incident Assignment process, continued

Process ID	Procedure or Decision	Description	Role
2.2.8	Incident		Analyst
SO 2.2.9	Reassign Incident to coordinator	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. The Incident Coordinator can decide whether to escalate the incident, reassign the incident, or close the incident.	Incident Analyst
SO 2.2.10	Create Major Incident Team	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.	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

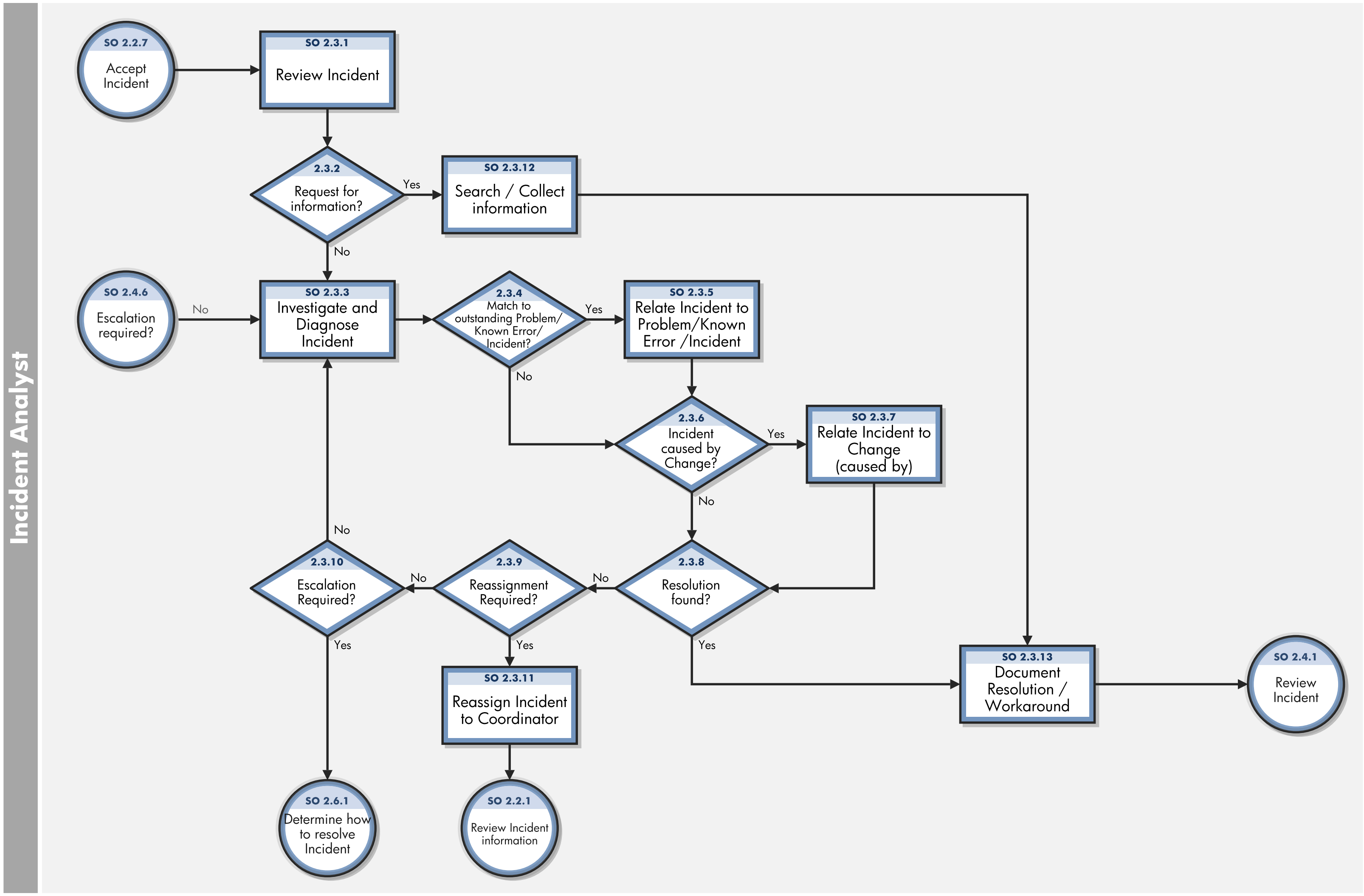
- Confirming the full impact of the incident, including the number and range of users affected
- Identifying any events that could have triggered the incident (for example, a recent change or user action)
- Searching known errors or the knowledgebase for a workaround or resolution
- Discovering any previous 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?
- 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.

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


Incident Analyst
SO 2.2.7 Accept Incident
SO 2.3.1 Review Incident
2.3.2 Request for information?
Yes
SO 2.3.12 Search / Collect information
No
SO 2.4.6 Escalation required?
No
SO 2.3.3 Investigate and Diagnose Incident
2.3.4 Match to outstanding Problem/ Known Error/ Incident?
Yes
SO 2.3.5 Relate Incident to Problem/Known Error /Incident
No
2.3.6 Incident caused by Change?
Yes
SO 2.3.7 Relate Incident to Change (caused by)
No
2.3.8 Resolution found?
No
2.3.9 Reassignment Required?
No
2.3.10 Escalation Required?
No
Yes
Yes
Yes
SO 2.3.11 Reassign Incident to Coordinator
SO 2.3.13 Document Resolution / Workaround
SO 2.4.1 Review Incident
SO 2.6.1 Determine how to resolve Incident
SO 2.2.1 Review Incident information

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 it is a RFI, continue with SO 2.3.12. If it is a service disruption, 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)

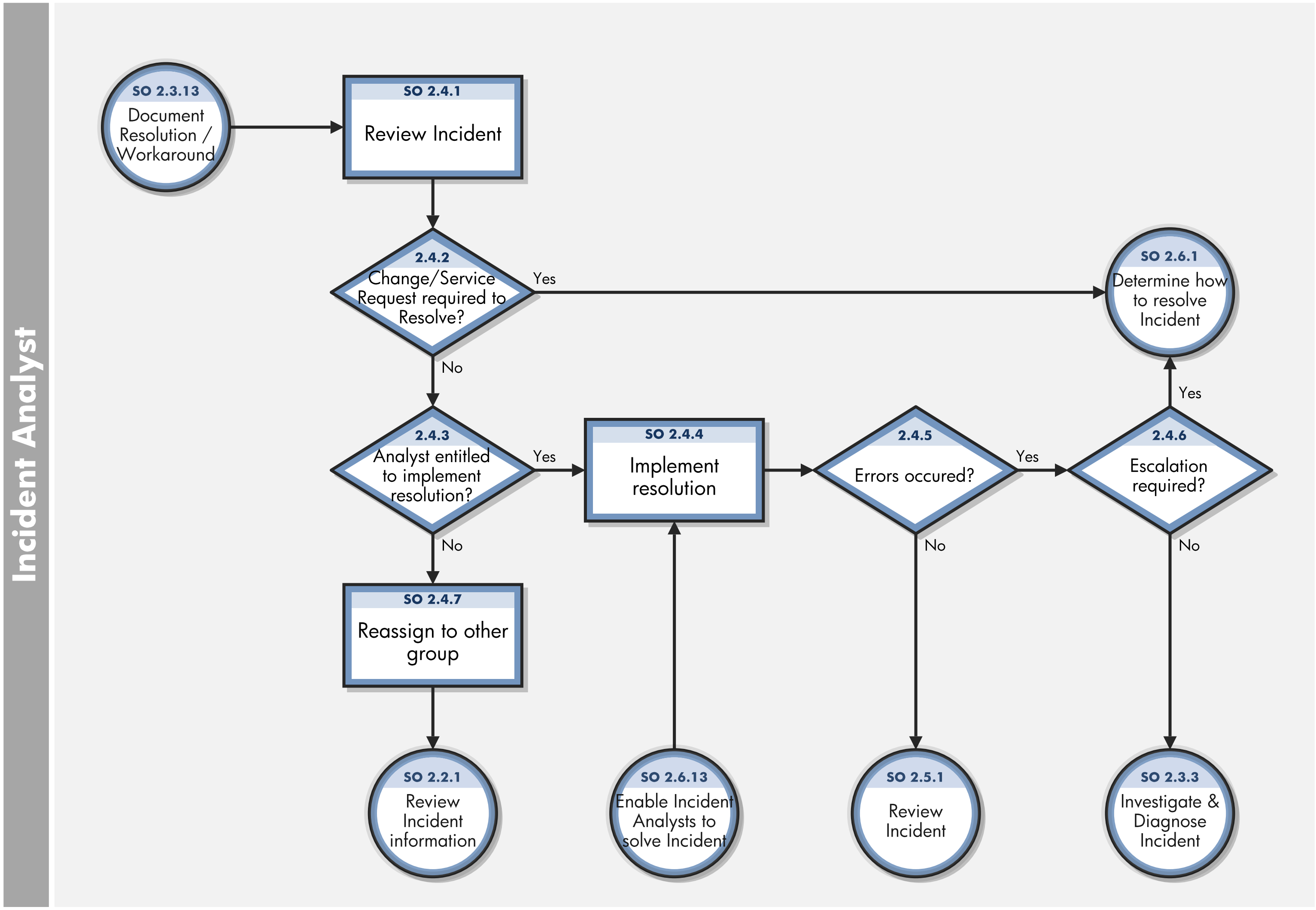
As part of the Incident Resolution and Recovery process, the Incident Analyst identifies and evaluates potential resolutions before those resolutions are applied and escalates incidents as necessary. The Incident Analyst may escalate an incident to the Incident Coordinator, including those incidents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

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


Incident Analyst
SO 2.3.13
Document Resolution / Workaround
SO 2.4.1
Review Incident
2.4.2
Change/Service Request required to Resolve?
Yes
No
SO 2.6.1
Determine how to resolve Incident
2.4.3
Analyst entitled to implement resolution?
Yes
No
SO 2.4.4
Implement resolution
2.4.5
Errors occured?
Yes
No
2.4.6
Escalation required?
Yes
No
SO 2.4.7
Reassign to other group
SO 2.2.1
Review Incident information
SO 2.6.13
Enable Incident Analysts to solve Incident
SO 2.5.1
Review Incident
SO 2.3.3
Investigate & Diagnose Incident

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

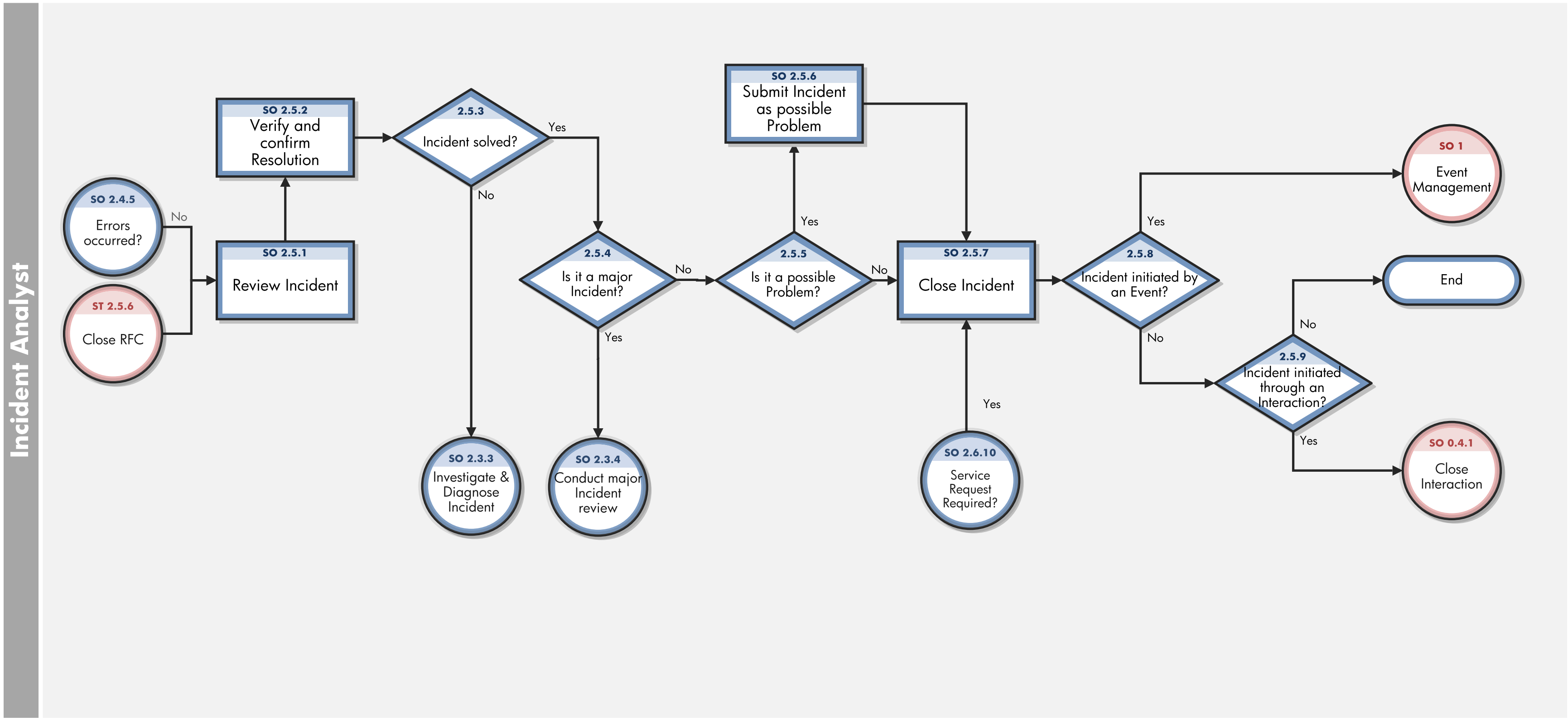
Incident Review and Closure (process SO 2.5)

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, the likelihood of the incident recurring is determined and Problem Candidate is selected accordingly.

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

The Incident Review and Closure workflow is illustrated in the following figure:


Incident Analyst
SO 2.4.5 Errors occurred?
No
ST 2.5.6 Close RFC
SO 2.5.1 Review Incident
SO 2.5.2 Verify and confirm Resolution
2.5.3 Incident solved?
Yes
No
SO 2.3.3 Investigate & Diagnose Incident
2.5.4 Is it a major Incident?
No
Yes
SO 2.3.4 Conduct major Incident review
2.5.5 Is it a possible Problem?
Yes
No
SO 2.5.6 Submit Incident as possible Problem
SO 2.5.7 Close Incident
Yes
SO 2.6.10 Service Request Required?
2.5.8 Incident initiated by an Event?
Yes
No
SO 1 Event Management
2.5.9 Incident initiated through an Interaction?
No
Yes
End
SO 0.4.1 Close Interaction

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 major Incident?	Major incident requires additional review at the stage. If it is a major incident, problem management activities may need to be undertaken to identify the root cause and take appropriate actions and plans to prevent future major incidents from occurring.	Incident Analyst
SO 2.5.5	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 2.5.6	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 2.5.7	Close Incident	The Incident Analyst closes the incident and selects the applicable resolution code.	Incident Analyst
SO 2.5.8	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 2.5.9	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.

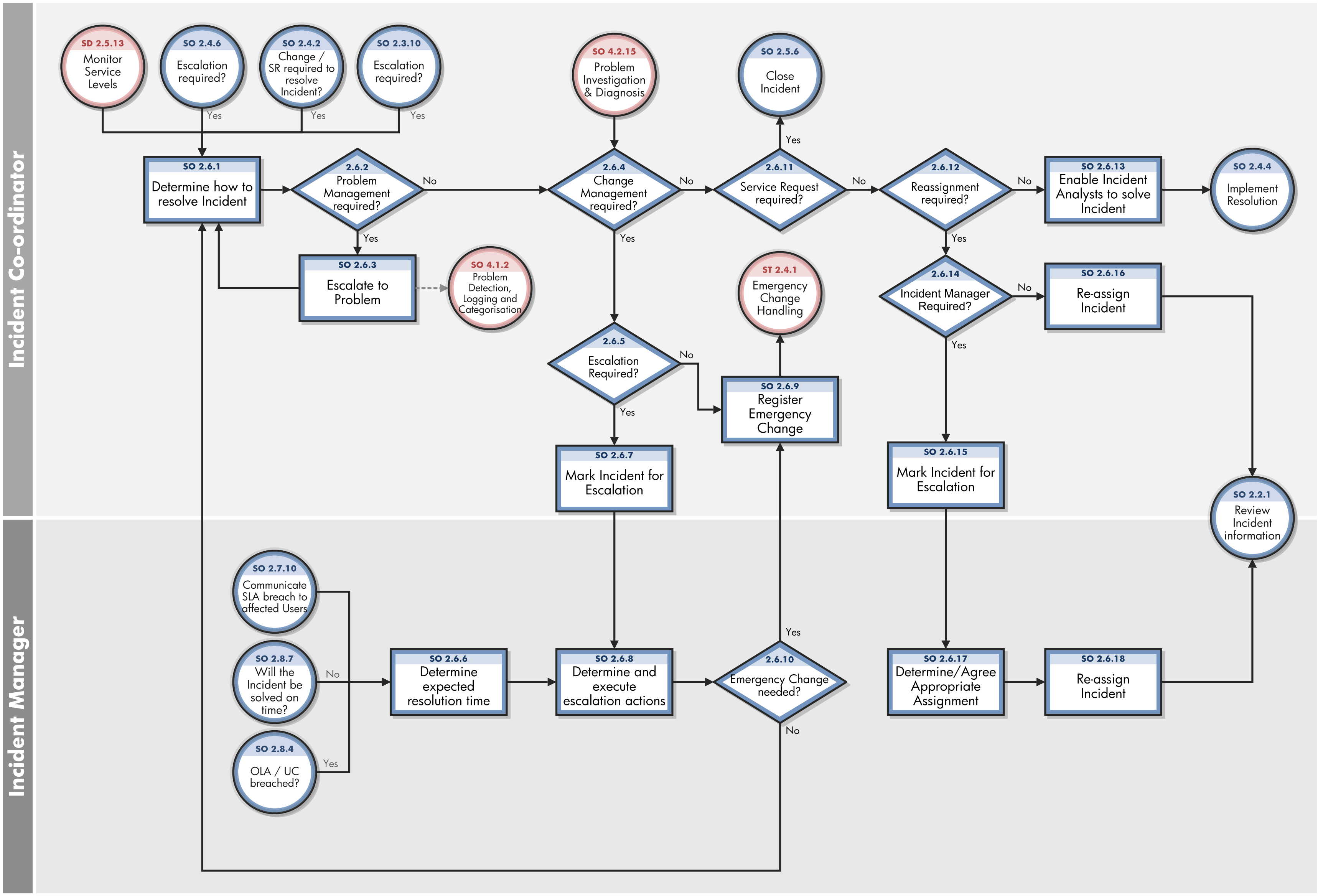
Incidents are escalated when the Incident Investigation and Diagnosis process or Incident Resolution and Recovery process exceeds SLA targets or if these targets are likely not to be met. If the steps to resolve an incident are taking too long or proving too difficult, the Incident Coordinator determines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

The Incident Escalation workflow is illustrated in the following figure:


Incident Co-ordinator
Incident Manager
SD 2.5.13 Monitor Service Levels
SO 2.4.6 Escalation required?
SO 2.4.2 Change / SR required to resolve Incident?
SO 2.3.10 Escalation required?
Yes
Yes
Yes
SO 2.6.1 Determine how to resolve Incident
2.6.2 Problem Management required?
No
Yes
SO 2.6.3 Escalate to Problem
SO 4.1.2 Problem Detection, Logging and Categorisation
SO 4.2.15 Problem Investigation & Diagnosis
2.6.4 Change Management required?
No
Yes
2.6.5 Escalation Required?
No
Yes
SO 2.6.7 Mark Incident for Escalation
SO 2.5.6 Close Incident
Yes
2.6.11 Service Request required?
No
ST 2.4.1 Emergency Change Handling
SO 2.6.9 Register Emergency Change
2.6.12 Reassignment required?
No
Yes
2.6.14 Incident Manager Required?
No
Yes
SO 2.6.15 Mark Incident for Escalation
SO 2.6.13 Enable Incident Analysts to solve Incident
SO 2.4.4 Implement Resolution
SO 2.6.16 Re-assign Incident
SO 2.2.1 Review Incident information
SO 2.7.10 Communicate SLA breach to affected Users
SO 2.8.7 Will the Incident be solved on time?
No
SO 2.8.4 OLA / UC breached?
Yes
SO 2.6.6 Determine expected resolution time
SO 2.6.8 Determine and execute escalation actions
2.6.10 Emergency Change needed?
Yes
No
SO 2.6.17 Determine/Agree Appropriate Assignment
SO 2.6.18 Re-assign Incident

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	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	Incident Manager

Incident Escalation process, continued

Process ID	Procedure or Decision	Description	Role
	actions	stakeholders.	
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

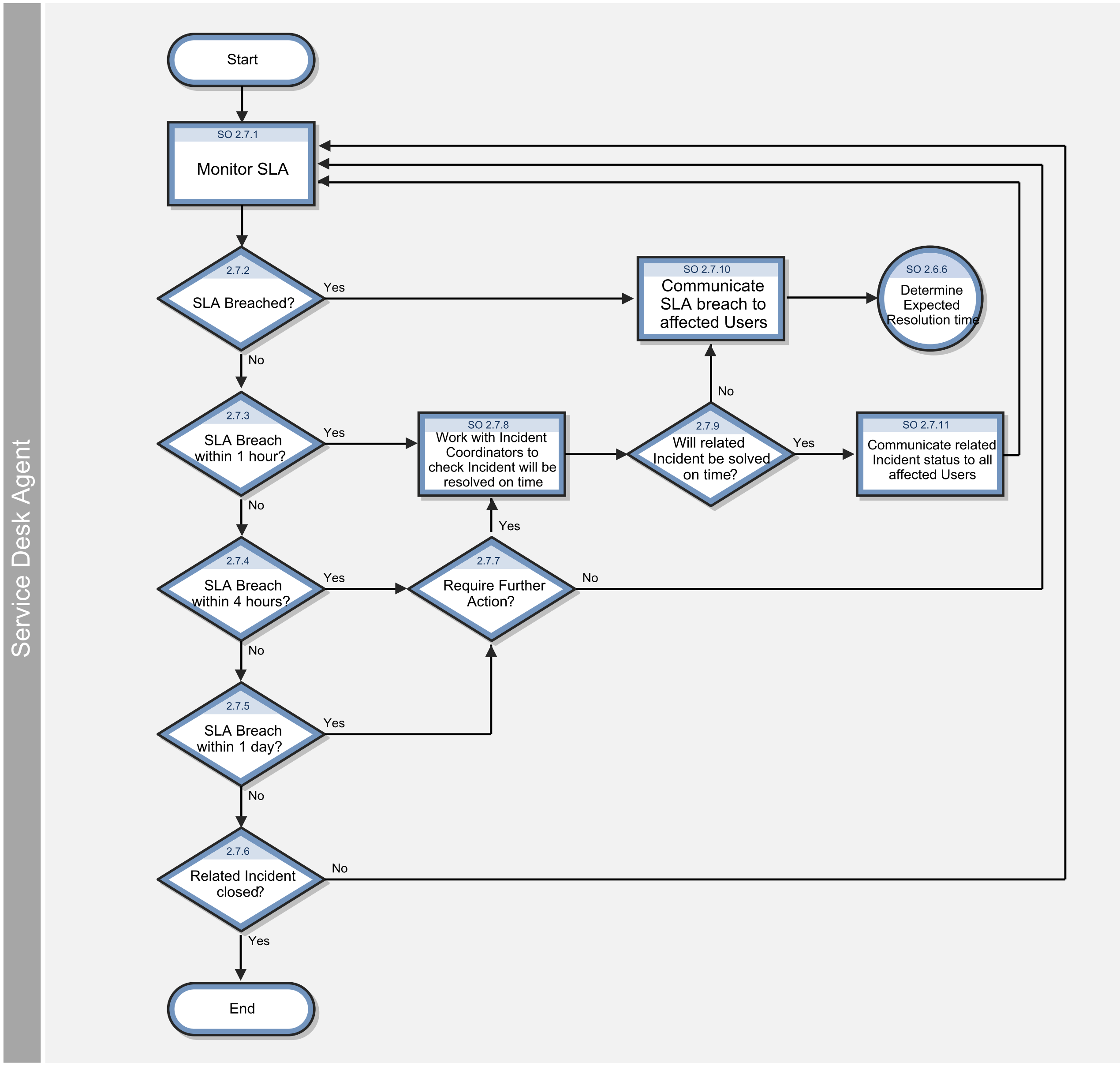
Process ID	Procedure or Decision	Description	Role
SO 2.6.17	Determine/ Agree appropriate assignment	The Incident Manager reviews the Incident to determine the appropriate Assignment Group based on the skills/ knowledge or permissions required to resolve the Incident.	Incident Manager
SO 2.6.18	Reassign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

The SLA Monitoring workflow is illustrated in the following figure:


Service Desk Agent
Start
SO 2.7.1
Monitor SLA
2.7.2
SLA Breached?
Yes
No
SO 2.7.10
Communicate SLA breach to affected Users
SO 2.6.6
Determine Expected Resolution time
2.7.3
SLA Breach within 1 hour?
Yes
No
SO 2.7.8
Work with Incident Coordinators to check Incident will be resolved on time
2.7.9
Will related Incident be solved on time?
No
Yes
SO 2.7.11
Communicate related Incident status to all affected Users
2.7.4
SLA Breach within 4 hours?
Yes
No
2.7.7
Require Further Action?
Yes
No
2.7.5
SLA Breach within 1 day?
Yes
No
2.7.6
Related Incident closed?
No
Yes
End

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

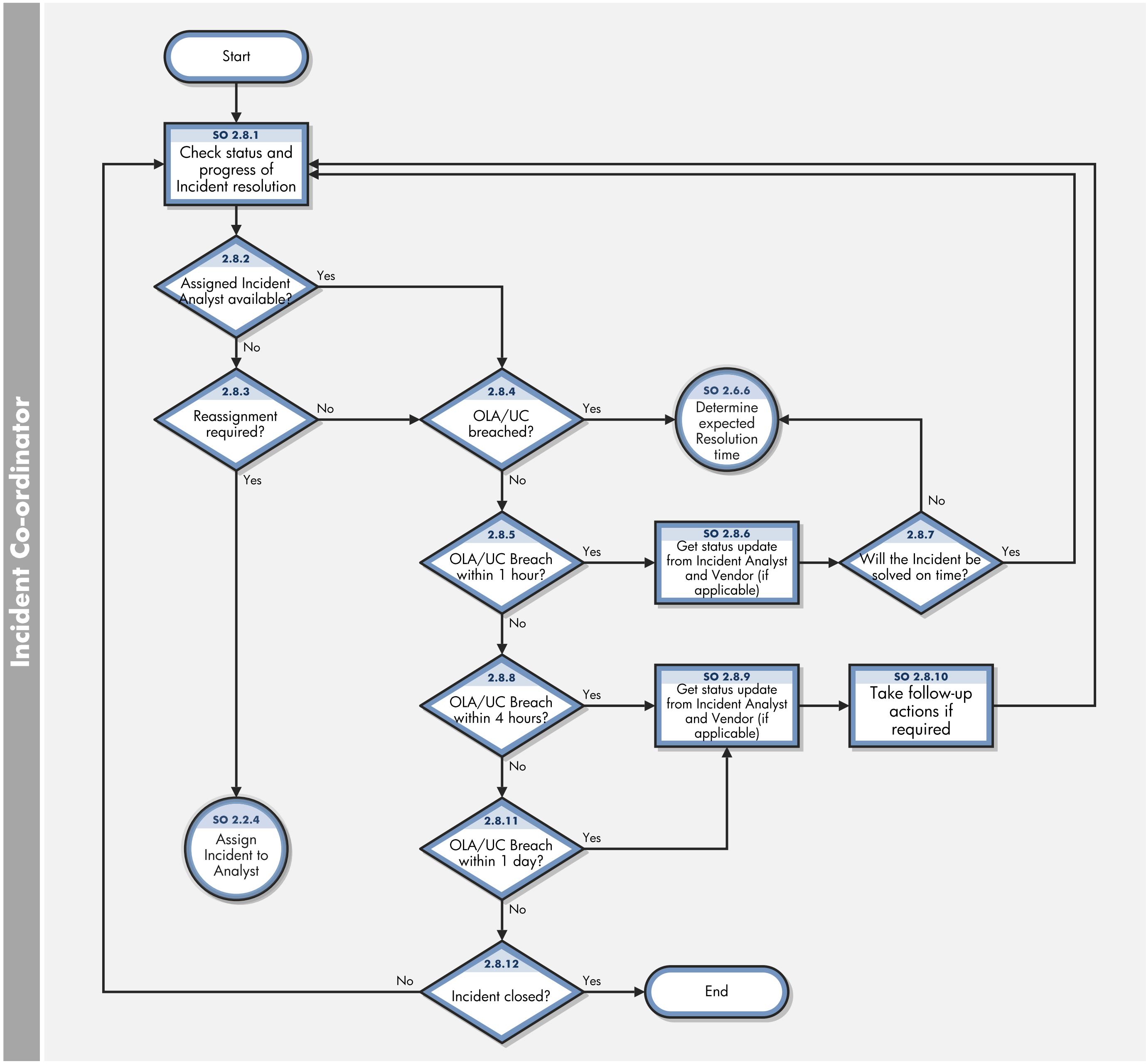
OLA and UC Monitoring (process SO 2.8)

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.

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


Incident Co-ordinator
Start
SO 2.8.1
Check status and progress of Incident resolution
2.8.2
Assigned Incident Analyst available?
Yes
No
2.8.3
Reassignment required?
No
Yes
2.8.4
OLA/UC breached?
Yes
No
SO 2.6.6
Determine expected Resolution time
2.8.5
OLA/UC Breach within 1 hour?
Yes
No
SO 2.8.6
Get status update from Incident Analyst and Vendor (if applicable)
2.8.7
Will the Incident be solved on time?
No
Yes
2.8.8
OLA/UC Breach within 4 hours?
Yes
No
SO 2.8.9
Get status update from Incident Analyst and Vendor (if applicable)
SO 2.8.10
Take follow-up actions if required
SO 2.2.4
Assign Incident to Analyst
2.8.11
OLA/UC Breach within 1 day?
Yes
No
2.8.12
Incident closed?
No
Yes
End

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
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	Incident Coordinator

OLA and UC Monitoring process, continued

Process ID	Procedure or Decision	Description	Role
		required actions.	
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

Chapter 7: Incident Management Details

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

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

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

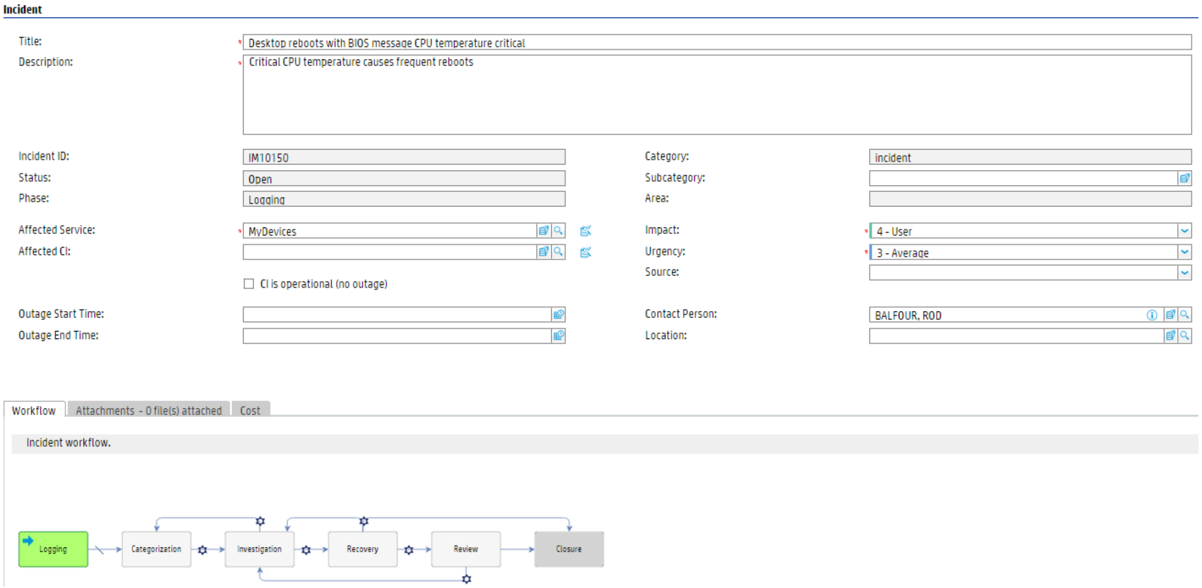
Topics in this section include:

- "Incident form after escalation from Service Desk" below
- "Categorize incident form" on the next page
- "Investigate incident form" on page 94
- "Recover incident form" on page 95
- "Review incident form" on page 95
- "Incident Management form details" on page 96

Incident form after escalation from Service Desk

The Incident Coordinator reviews incidents opened 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 opened from Service Desk is illustrated in the following screenshot:



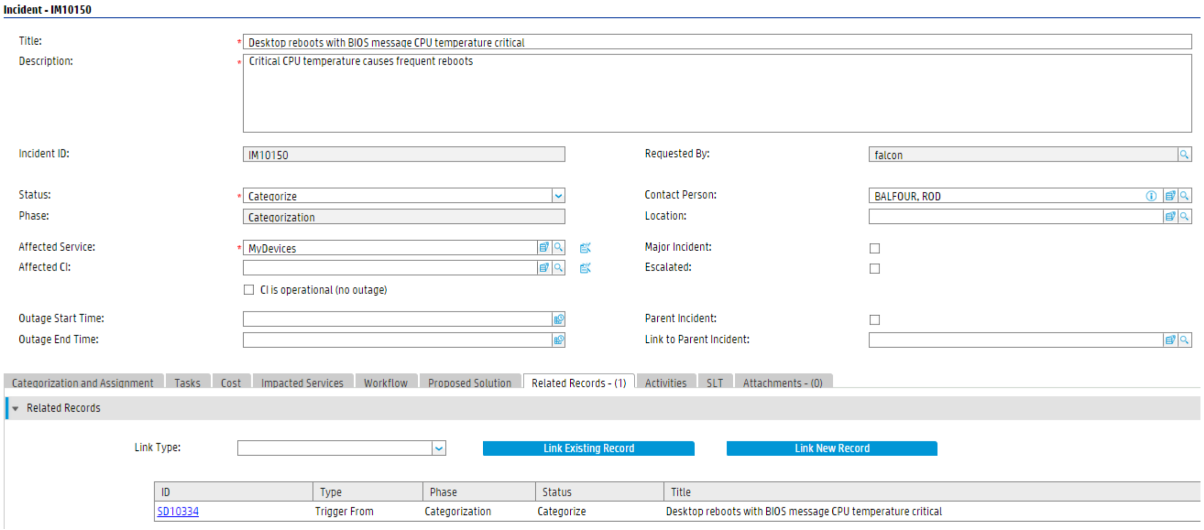
Incident

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Category:	incident
Status:	Open	Subcategory:	
Phase:	Logging	Area:	
Affected Service:	* MyDevices	Impact:	* 4 - User
Affected CI:		Urgency:	* 3 - Average
	□ CI is operational (no outage)	Source:	
Outage Start Time:		Contact Person:	BALFOUR, ROD
Outage End Time:		Location:	

Workflow | Attachments - 0 file(s) attached | Cost

Incident workflow.

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



Incident - IM10150

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Requested By:	falcon
Status:	* Categorize	Contact Person:	BALFOUR, ROD
Phase:	Categorization	Location:	
Affected Service:	* MyDevices	Major Incident:	□
Affected CI:		Escalated:	□
	□ CI is operational (no outage)		
Outage Start Time:		Parent Incident:	□
Outage End Time:		Link to Parent Incident:	

Categorization and Assignment | Tasks | Cost | Impacted Services | Workflow | Proposed Solution | Related Records - (1) | Activities | SLT | Attachments - (0)

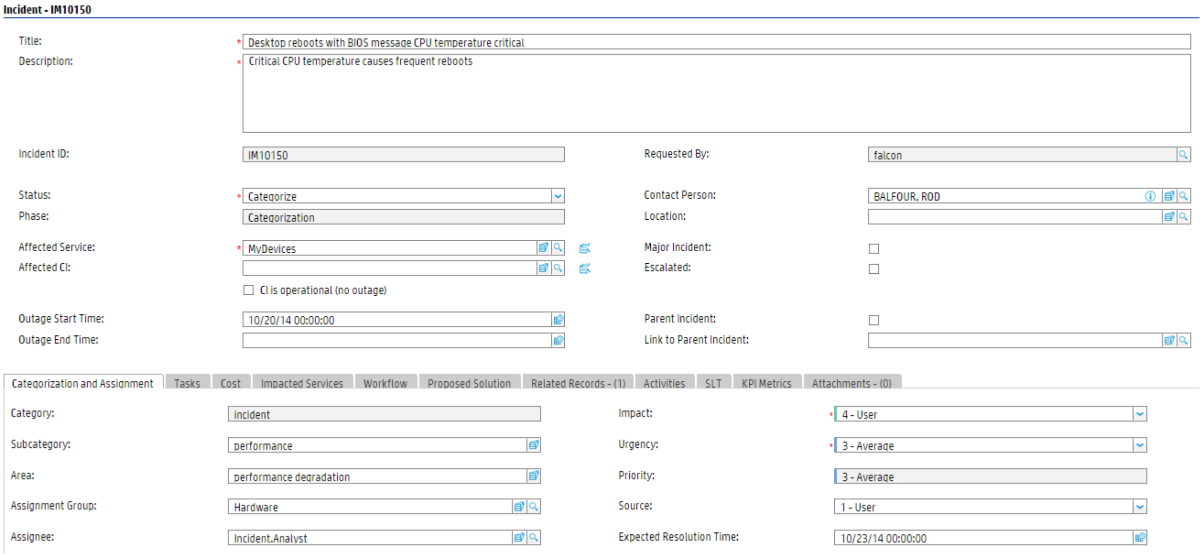
Related Records

Link Type:

ID	Type	Phase	Status	Title
SD10334	Trigger 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.



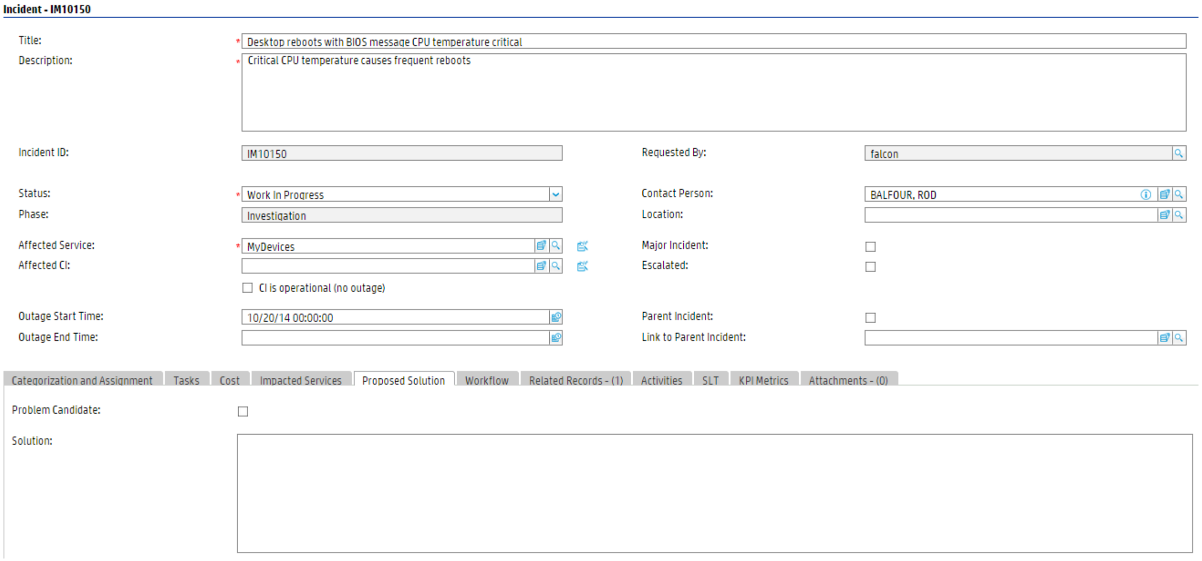
Incident - IM10150

Title:	Desktop reboots with BIOS message CPU temperature critical		
Description:	Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Requested By:	falcon
Status:	Categorize	Contact Person:	BALFOUR, ROD
Phase:	Categorization	Location:	
Affected Service:	MyDevices	Major Incident:	□
Affected CI:		Escalated:	□
	□ CI is operational (no outage)		
Outage Start Time:	10/20/14 00:00:00	Parent Incident:	□
Outage End Time:		Link to Parent Incident:	

Category:	incident	Impact:	4 - User
Subcategory:	performance	Urgency:	3 - Average
Area:	performance degradation	Priority:	3 - Average
Assignment Group:	Hardware	Source:	1 - User
Assignee:	Incident.Analyst	Expected Resolution Time:	10/23/14 00:00:00

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.



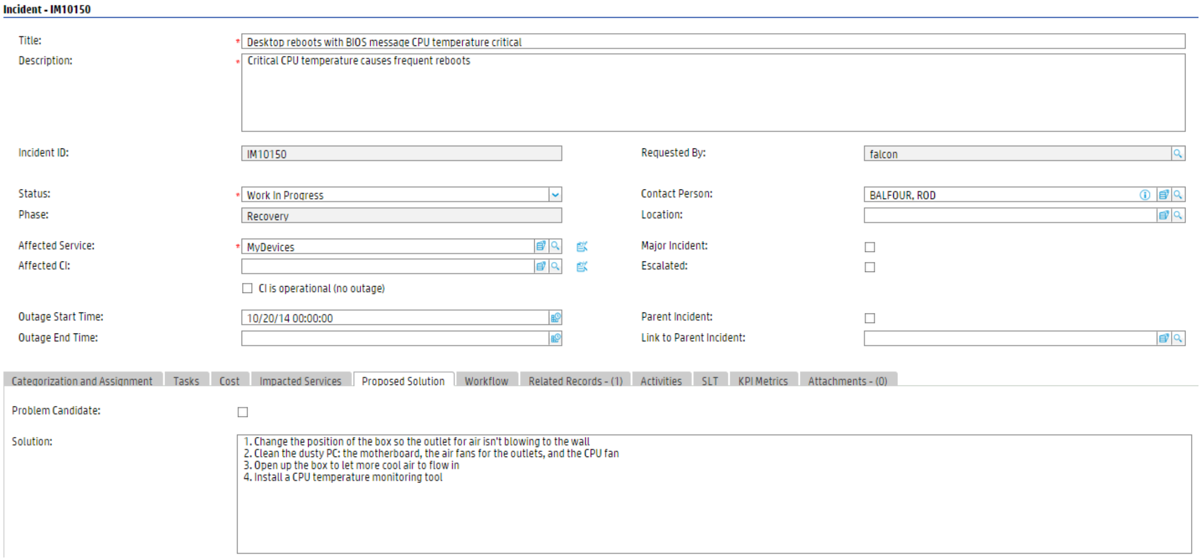
Incident - IM10150

Title:	Desktop reboots with BIOS message CPU temperature critical		
Description:	Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Requested By:	falcon
Status:	Work In Progress	Contact Person:	BALFOUR, ROD
Phase:	Investigation	Location:	
Affected Service:	MyDevices	Major Incident:	□
Affected CI:		Escalated:	□
	□ CI is operational (no outage)		
Outage Start Time:	10/20/14 00:00:00	Parent Incident:	□
Outage End Time:		Link to Parent Incident:	

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.



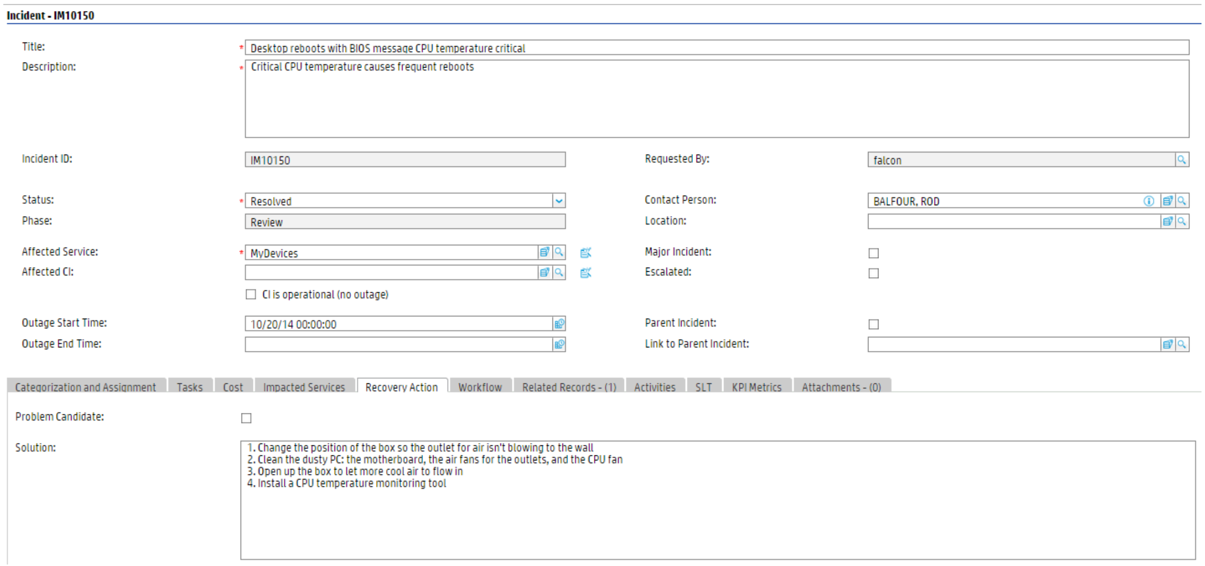
Incident - IM10150

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Requested By:	falcon
Status:	* Work In Progress	Contact Person:	BALFOUR, ROD
Phase:	Recovery	Location:	
Affected Service:	* MyDevices	Major Incident:	□
Affected CI:		Escalated:	□
	□ CI is operational (no outage)		
Outage Start Time:	10/20/14 00:00:00	Parent Incident:	□
Outage End Time:		Link to Parent Incident:	

Problem Candidate:	□
Solution:	1. Change the position of the box so the outlet for air isn't blowing to the wall 2. Clean the dusty PC: the motherboard, the air fans for the outlets, and the CPU fan 3. Open up the box to let more cool air to flow in 4. Install a CPU temperature monitoring tool

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 - IM10150

Title:	* Desktop reboots with BIOS message CPU temperature critical		
Description:	* Critical CPU temperature causes frequent reboots		
Incident ID:	IM10150	Requested By:	falcon
Status:	* Resolved	Contact Person:	BALFOUR, ROD
Phase:	Review	Location:	
Affected Service:	* MyDevices	Major Incident:	□
Affected CI:		Escalated:	□
	□ CI is operational (no outage)		
Outage Start Time:	10/20/14 00:00:00	Parent Incident:	□
Outage End Time:		Link to Parent Incident:	

Problem Candidate:	□
Solution:	1. Change the position of the box so the outlet for air isn't blowing to the wall 2. Clean the dusty PC: the motherboard, the air fans for the outlets, and the CPU fan 3. Open up the box to let more cool air to flow in 4. Install a CPU temperature monitoring tool

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	A short description that summarizes the incident. This field is prepopulated with data from an escalated interaction. This is a required field.
Description	A detailed description of the incident. This field is prepopulated with data from an escalated interaction. This is a required field.
Phase	This is a system-generated field. These phases are available out-of-box: • Logging • Categorization • Investigation • Recovery • Review • Closure
Status	Displays the status of the incident. These statuses are available out-of-box: • 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 Parent Incident — The incident has been linked to a parent incident and waiting for the resolution of the parent incident. This status is automatically set when an incident is linked to a parent incident. • Pending Other — You need something from an outside source other than

Incident Management form details, continued

Label	Description
	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	The service affected by this incident. This field is populated with data from the interaction record. See "Service Desk Interaction Management form details" on page 42 for additional information. This is a required field.
Affected CI	The configuration item (CI) that is affecting the service negatively. This field is populated with data from the interaction record. See "Service Desk Interaction Management form details" on page 42 for additional information. 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.
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

Incident Management form details, continued

Label	Description
	outage time.
Category	This field describes the type of incident, based on ITIL service-centric processes. This field is prepopulated with data from the escalated interaction. This is a required field. A workflow is bound to a category. You must select a category before opening an incident form if the incident is not opened from an interaction and there is no default category specified. 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. The following categories are available for the out-of-box incidents: • Complaint • Incident • Request for administration • Request for information
Subcategory	This field is prepopulated with the data from the interaction from which the incident is opened. The subcategory selections depend on the category. This is a required field when phase starts from Categorization. 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 42 and "Interaction categories" on page 48.
Area	The third level of classifying an interaction, mainly used for reporting purposes. This field is prepopulated with the data from the interaction from which the incident is opened. 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 48. 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 42.
Impact	This field is prepopulated with data from an escalated interaction. It specifies the impact the incident has on the business. The impact and the urgency are used to calculate the priority. These impacts are available out-of-box: • Enterprise

Incident Management form details, continued

Label	Description
	• Site/Dept • Multiple Users • User
Urgency	This field is prepopulated with data from an escalated interaction. The urgency indicates how pressing the incident is for the organization. The urgency and the impact are used to calculate the priority. For additional information, see"Service Desk Interaction Management form details" on page 42.
Priority	The order in which to address this incident in comparison to others. The priority value is calculated using initial impact and urgency. This field only appears for incidents being updated or escalated from interactions.
Major Incident	If selected (set to true), this field indicates that the issue is a major issue, which requires informing the specified Incident Manager, and imputing review details under the Major Incident Review section.
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 incident. This field ensures that the correct person will be notified about updates to the incident. 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.
Source	The source from which the Incident is reported. The following out-of-box sources are available: • User • Group • Event • Incident
Parent Incident	If selected (set to true), this field indicates that the incident is a parent incident, that allows other incidents link to it for issue classification, and the child

Incident Management form details, continued

Label	Description
	incidents can be viewed under Child Incidents section. If unselected later after being selected, all the linked child incidents are unlinked. Once an incident is set as a parent incident, it cannot be linked to a parent incident any longer.
Link to Parent Incident	The ID of the parent incident. This field can be populated with incident ID based on predefined query for parent incidents. One incident can only be linked to one parent incident. Once linked to a parent incident, this incident cannot be set as parent incident any longer.
Categorization and Assignment section > Assignment Group	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. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. **Tip:** You may want to adapt the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail • Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support

Incident Management form details, continued

Label	Description
	• Service Desk • Service Manager This is a required field.
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	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: • Task ID • Status • Phase • Priority • Title
Cost section	The user can add cost details of parts and labor for incident handling. For parts cost, the user needs to add expense lines with the part number from product catalog and the quantity that have been used during the incident handling. For labor cost, the user needs to add technicians who have been working on the incident with the working hours. Select a currency for cost calculation, then the total cost of the incident will be calculated by the system.
Activities > Vendor/Supplier	The name of the vendor/supplier the incident is assigned to. Used when a vendor/supplier needs to be involved in fixing the incident.
Activities > Vendor/Supplier Record	This number refers to the incident number from the vendor/supplier logging system. This is an informational field for reference only. This field is only visible when incident status is Pending Vendor/Supplier.

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: • Caused By Incidents • Caused Incidents • Caused By Changes • Related Interactions • Related Problems • Related Known Errors • Related Requests
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: • 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.
Proposed Solution/Recovery Action section > Problem	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

Incident Management form details, continued

Label	Description
Candidate	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.
Closure Code	Specifies a predefined closure code to describe how the incident has been resolved. The out-of-box options in this field are based on customer reference data. **Tip:** You may want to tailor these options to match your business needs. These closure codes are available out-of-box: • Not Reproducible • Out of Scope • Request Rejected • Solved by Change/Service Request • Solved by User Instruction • Solved by Workaround • Unable to Solve • Withdrawn by User • No Fault Found • No User Response • Resolved Successfully • Diagnosed Successfully
Completion Comments	This field is to document additional comments to close the incident.
Affected Services	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.
SLT >	This subsection provides a list of process SLTs related to the incident. The

Incident Management form details, continued

Label	Description
Process Targets	information includes Agreement name, status, SLT name, From and To specifications for the Agreement, and Expiration. Similar information is available for interactions, problems, and changes.
SLT > Uptime Targets	This subsection displays uptime availability data for the SLTs related to the incident. The data displayed includes the following information: • Status • SLT name • Required Monthly Uptime (%) • Withdrawn by User • Current Uptime this Month (%) • Next Expiration • Affected CI • SLT ID Similar information is available for interactions, problems, and changes.
SLT > Max Duration Targets	This subsection displays duration availability data for the SLTs related to the incident. The data displayed includes the following information: • Status • SLT name • Total outages this month • Average outage duration • Next expiration • Affected CI • SLT ID Similar information is available for interactions, problems, and changes.
SLT > Upcoming Alerts	This subsection displays all upcoming Agreement alerts to help users prioritize the incidents needing attention.

Incident Management form details, continued

Label	Description
	The data displayed includes the following information: • Alert name • SLT name • Alert time **Note:** For additional information, see the online Help topic, Service Level Agreement alerts.

Chapter 8: 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 109
- "Input and output of Problem Management" on page 114
- "Key Performance Indicators for Problem Management" on page 116
- "RACI matrix for Problem Management" on page 118

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 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 out-of-box workflows for problems (the “Problem” workflow) and known errors (the "Known Error" workflow). These workflows are associated respectively with the out-of-box "problem" and "known error" categories. The workflows ensure 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 with that 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.

Note: There are no out-of-box tasks for Known Error records.

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.

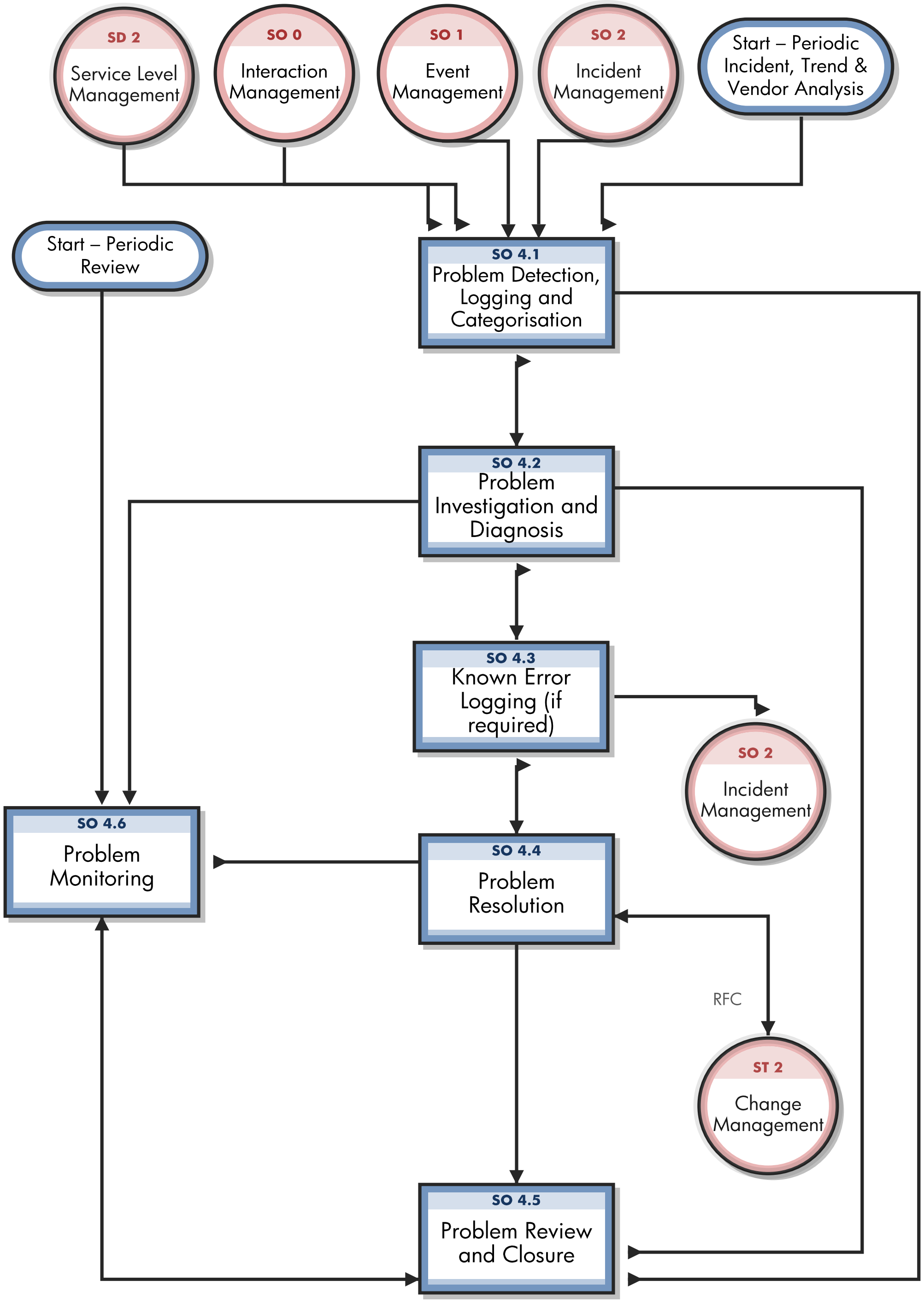
Problem management process overview

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.

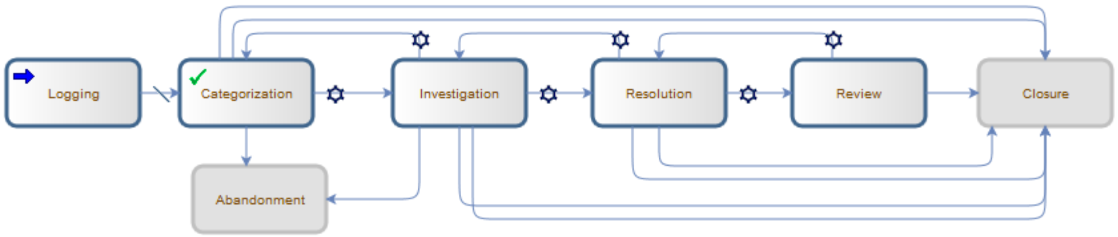
The following figure provides a general overview of the problem management processes and workflows. These workflows are described in detail in "Problem Management Workflows" on page 120.


SD 2
Service Level Management
SO 0
Interaction Management
SO 1
Event Management
SO 2
Incident Management
Start – Periodic Incident, Trend & Vendor Analysis
Start – Periodic Review
SO 4.1
Problem Detection, Logging and Categorisation
SO 4.2
Problem Investigation and Diagnosis
SO 4.3
Known Error Logging (if required)
SO 2
Incident Management
SO 4.6
Problem Monitoring
SO 4.4
Problem Resolution
RFC
ST 2
Change Management
SO 4.5
Problem Review and Closure

Problem management phases

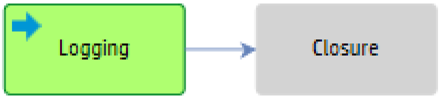
Service Manager uses phases to describe the steps needed to resolve a problem. The phase also determines the forms users see, the actions users can manually trigger. In an out-of-box system, most of the phase transitions are triggered by change to the problem status.

The following figure shows the workflow phases for a problem.



The out-of-box known error workflow uses only two phases to differentiate the open and closed known error records. A known error is opened with a documented root cause and workaround, and closed when a permanent solution is found.

The following figure shows the workflow phases for a known error:



Problem Management user roles

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

Problem Management user roles

Role	Responsibilities
Problem Manager	• 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	• Periodically perform analysis to see if new problems need to be registered • Register problems • Categorize and prioritize problems

Problem Management user roles , continued

Role	Responsibilities
	• Assign work to the Problem Analysts • Schedule the problem resolution • Coordinate root cause analysis and diagnosis Identify and raise known errors
Problem Analyst	• 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 major problems and ensure problem manager is notified • 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
• 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)	• Problems • Known errors • Workarounds

Input and output for Problem Management, continued

Input to Problem Management	Output from Problem Management
• 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 ○ 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) ○ Suspicion or detection of a cause of one or more incidents by the Service Desk, resulting in the creation of a problem record. • Event management ○ Trend analysis and review of events (for example, performance events) ○ Error logs • Configuration management ○ Configuration details and relationships (service model)	• Problem reports (for example, status updates, trends, and performance) • RFCs (to remove infrastructure errors) **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.

Input and output for Problem Management, continued

Input to Problem Management	Output from Problem Management
• Change management ◦ RFC and change request status, approval and closure. • Security management ◦ Notification of potential security breaches that require resolution • Suppliers (external providers) • Notification of problems from suppliers/vendors	

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 2011 and COBIT 4.1 KPIs are included below.

ITIL 2011 Key Performance Indicators

The following are ITIL 2011 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 9: 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 125
- "Problem Resolution (process SO 4.3)" on page 130
- "Problem Review and Closure (process SO 4.4)" on page 136
- "Problem and Known Error Monitoring (process SO 4.5)" on page 140

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.

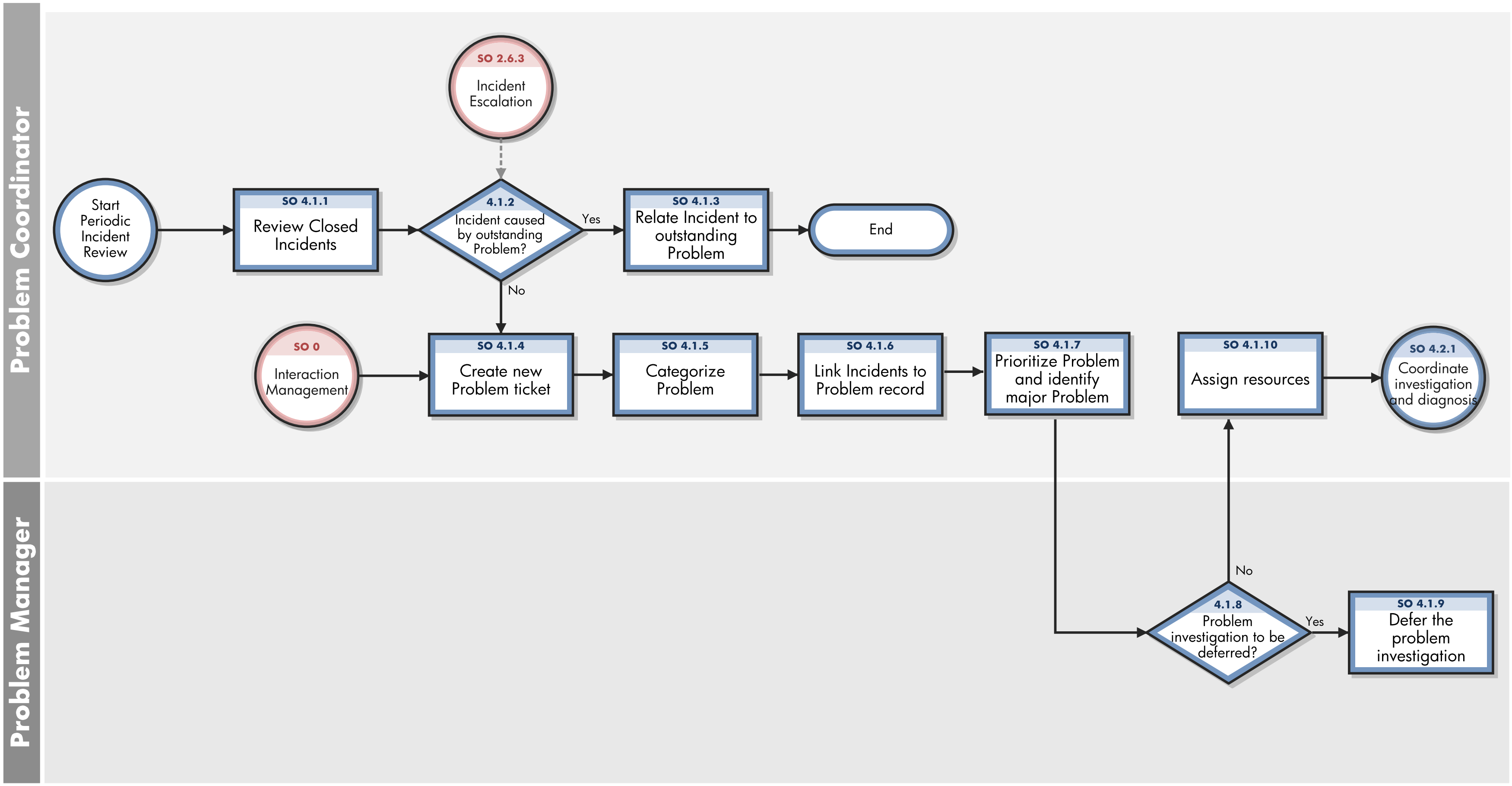
The Problem Detection, Logging, and Categorization process should include reference to information that assists analysis, such as:

- 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) or interaction(s) that initiated the problem should be referenced, and relevant details copied from the incident(s) or interaction(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 Coordinator
Problem Manager
SO 2.6.3
Incident Escalation
Start Periodic Incident Review
SO 4.1.1
Review Closed Incidents
4.1.2
Incident caused by outstanding Problem?
Yes
SO 4.1.3
Relate Incident to outstanding Problem
End
No
SO 0
Interaction Management
SO 4.1.4
Create new Problem ticket
SO 4.1.5
Categorize Problem
SO 4.1.6
Link Incidents to Problem record
SO 4.1.7
Prioritize Problem and identify major Problem
SO 4.1.10
Assign resources
SO 4.2.1
Coordinate investigation and diagnosis
No
4.1.8
Problem investigation to be deferred?
Yes
SO 4.1.9
Defer the problem investigation

Problem Detection, Logging, and Categorization process

Process ID	Procedure or Decision	Description	Role
SO 4.1.1	Review closed incidents	Periodically, the Problem Coordinator must review the closed incidents to detect new problems or 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: • 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 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).	Problem Coordinator
SO 4.1.2	Incident caused by outstanding problem?	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.	Problem Coordinator
SO 4.1.3	Relate incident to outstanding problem	If the incident is caused by an outstanding problem, the incident must be linked to the problem. If required, the problem is updated and the Problem Analyst is notified (for example, when a workaround has been applied).	Problem Coordinator
SO 4.1.4	Create new problem ticket	Create a new problem ticket that captures all the relevant data, such as: • User details	Problem Coordinator

Problem Detection, Logging, and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
		• Configuration Item (CI) details • Date and time the problem was initially logged • Description • Details of all diagnostic or attempted recovery actions taken so far 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.	
SO 4.1.5	Categorize problem	The Problem Coordinator categorizes the problem into a specific domain (for example, hardware, software, or security). 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. If the problem is not categorized in the appropriate category, the Problem Coordinator can change the category, which initiates a new workflow.	Problem Coordinator
SO 4.1.6	Link incidents to problem record	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.	Problem Coordinator
SO 4.1.7	Prioritize problem and identify major problem	The Problem Coordinator identifies whether it is a major problem based on the impact and the organization's priority.	Problem Coordinator

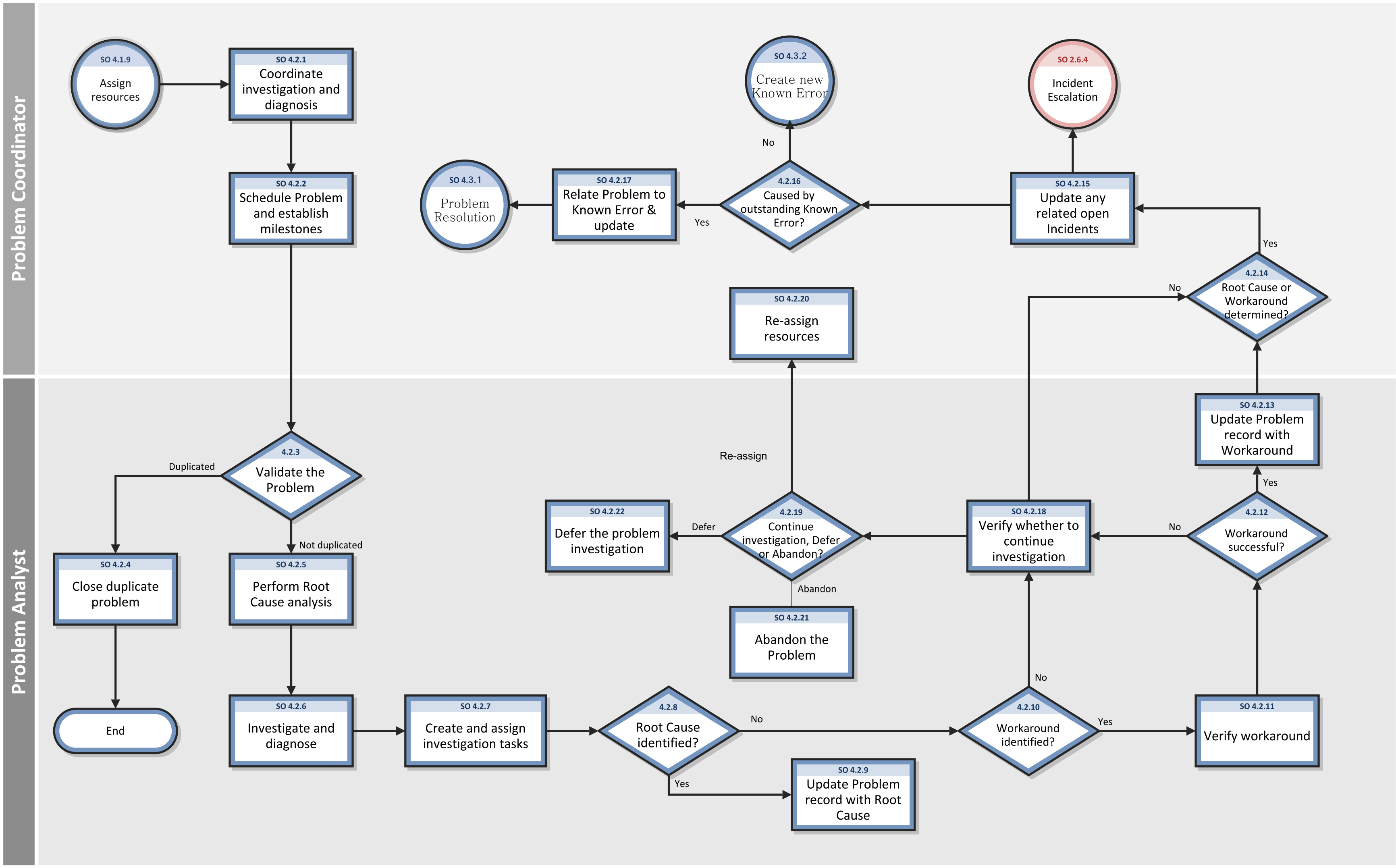
Problem Detection, Logging, and Categorization process, continued

Process ID	Procedure or Decision	Description	Role
SO 4.1.8	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 4.1.9	Defer the problem investigation	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. Reasons for deferring problem include the following: • 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 4.1.10	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 Coordinator
Problem Analyst
SO 4.1.9 Assign resources
SO 4.2.1 Coordinate investigation and diagnosis
SO 4.2.2 Schedule Problem and establish milestones
SO 4.3.1 Problem Resolution
SO 4.2.17 Relate Problem to Known Error & update
Yes
4.2.16 Caused by outstanding Known Error?
No
SO 4.3.2 Create new Known Error
SO 2.6.4 Incident Escalation
SO 4.2.15 Update any related open Incidents
Yes
No
4.2.14 Root Cause or Workaround determined?
SO 4.2.20 Re-assign resources
SO 4.2.13 Update Problem record with Workaround
Yes
4.2.3 Validate the Problem
Duplicated
Not duplicated
SO 4.2.4 Close duplicate problem
End
SO 4.2.5 Perform Root Cause analysis
SO 4.2.6 Investigate and diagnose
SO 4.2.7 Create and assign investigation tasks
4.2.8 Root Cause identified?
No
Yes
SO 4.2.9 Update Problem record with Root Cause
Re-assign
SO 4.2.22 Defer the problem investigation
Defer
4.2.19 Continue investigation, Defer or Abandon?
Abandon
SO 4.2.21 Abandon the Problem
SO 4.2.18 Verify whether to continue investigation
No
4.2.12 Workaround successful?
No
4.2.10 Workaround identified?
Yes
SO 4.2.11 Verify workaround

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
SO 4.2.5	Perform root cause analysis	The Problem Analyst performs root cause analysis of the problem. Root cause analysis can include the following methods: • Chronological Analysis • Pain Value Analysis • Kepner and Tregoe • Brainstorming • Ishikawa Diagrams	Problem Analyst

Problem Investigation and Diagnosis process, continued

Process ID	Procedure or Decision	Description	Role
		- Pareto Analysis	
SO 4.2.6	Investigate and diagnose	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. 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	Problem Analyst
SO 4.2.7	Create and assign investigation tasks	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.	Problem Analyst
SO 4.2.8	Root cause identified?	If the root cause is not identified, the Problem Analyst must determine whether there is a workaround for the problem. If a root cause is identified, the Problem Analyst updates the problem record with the details.	Problem Analyst
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

Problem Investigation and Diagnosis process, continued

Process ID	Procedure or Decision	Description	Role
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	Caused by outstanding known error?	Determine whether the root cause for this problem is related to an outstanding known error. If yes, continue with SO 4.2.xx. If no, forward the problem to the Problem Resolution phase, and then create a new known error record .	Problem Coordinator
SO 4.2.17	Relate problem to outstanding known error	The problem is moved to the Problem Resolution phase and linked to the existing known error record. The resolution of the problem is dependent on the resolution of this known error.	Problem Coordinator
SO 4.2.18	Verify whether to continue investigation	The Problem Analyst determines whether to continue with the investigation, start problem resolution, or recommend abandonment.	Problem Analyst
SO 4.2.19	Continue, defer, or abandon investigation?	If the Problem Analyst decides to continue the investigation, the workflow moves to SO 4.2.6. 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. If the problem can be abandoned, the workflow moves to SO 4.2.19.	Problem Analyst

Problem Investigation and Diagnosis process, continued

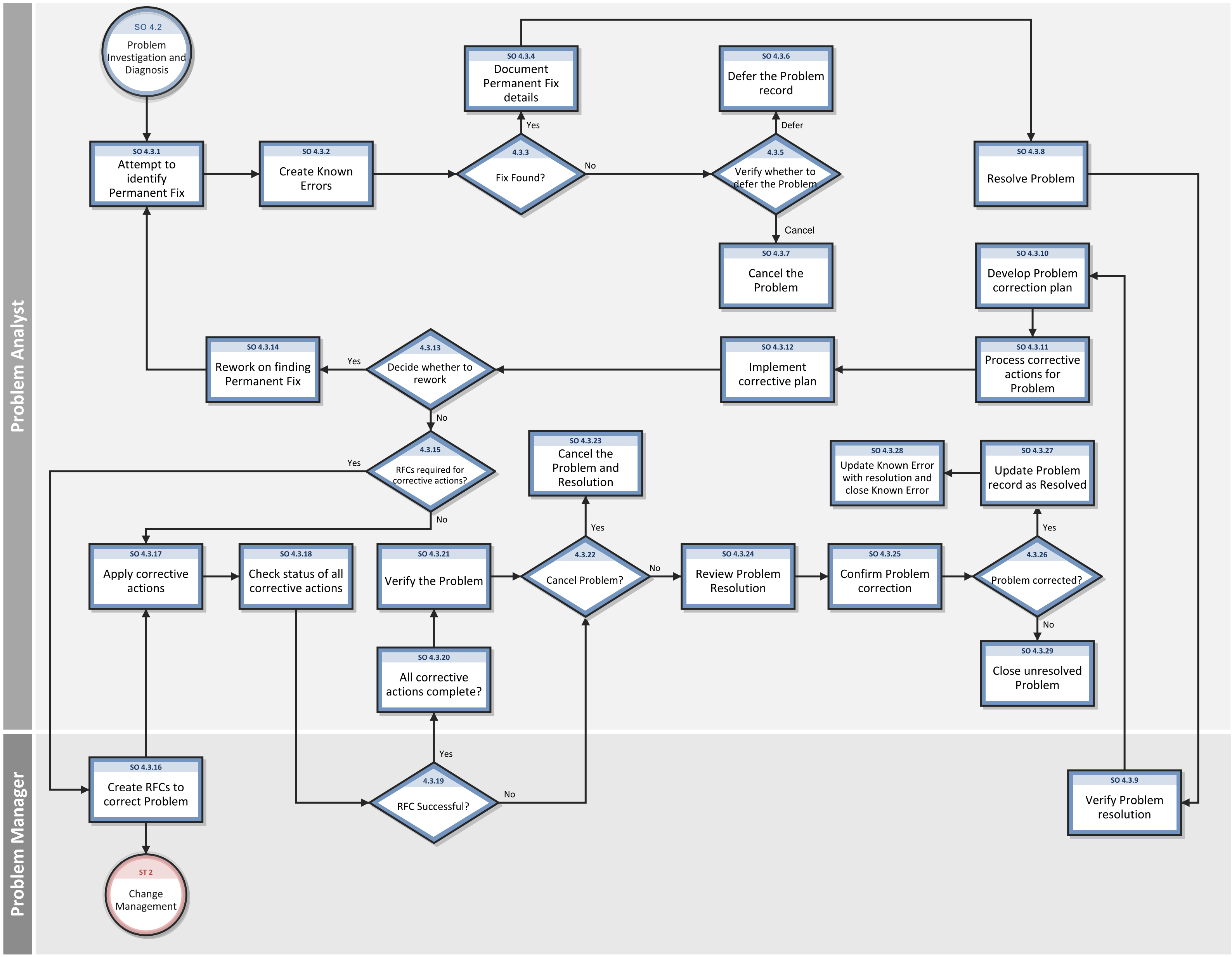
Process ID	Procedure or Decision	Description	Role
		If the problem can be deferred, the workflow moves to SO 4.2.20.	
SO 4.2.20	Re-assign resources	The Problem Coordinator needs to re-assigns the problem to other resource to continue the problem investigation. The problem is moved back to Categorization phase with the Assign status again, and the workflow moves to SO 4.1.10.	Problem Coordinator
SO 4.2.21	Abandon the problem	The Problem Analyst abandons the problem ticket.	Problem Analyst
SO 4.2.22	Defer the problem investigation	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. Reasons for deferring problem include the following: • 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 Analyst
Problem Manager
SO 4.2
Problem Investigation and Diagnosis
SO 4.3.1
Attempt to identify Permanent Fix
SO 4.3.2
Create Known Errors
4.3.3
Fix Found?
Yes
No
SO 4.3.4
Document Permanent Fix details
4.3.5
Verify whether to defer the Problem
Defer
Cancel
SO 4.3.6
Defer the Problem record
SO 4.3.7
Cancel the Problem
SO 4.3.8
Resolve Problem
SO 4.3.9
Verify Problem resolution
SO 4.3.10
Develop Problem correction plan
SO 4.3.11
Process corrective actions for Problem
SO 4.3.12
Implement corrective plan
4.3.13
Decide whether to rework
Yes
No
SO 4.3.14
Rework on finding Permanent Fix
4.3.15
RFCs required for corrective actions?
Yes
No
SO 4.3.16
Create RFCs to correct Problem
ST 2
Change Management
SO 4.3.17
Apply corrective actions
SO 4.3.18
Check status of all corrective actions
4.3.19
RFC Successful?
Yes
No
SO 4.3.20
All corrective actions complete?
SO 4.3.21
Verify the Problem
4.3.22
Cancel Problem?
Yes
No
SO 4.3.23
Cancel the Problem and Resolution
SO 4.3.24
Review Problem Resolution
SO 4.3.25
Confirm Problem correction
4.3.26
Problem corrected?
Yes
No
SO 4.3.27
Update Problem record as Resolved
SO 4.3.28
Update Known Error with resolution and close Known Error
SO 4.3.29
Close unresolved Problem

Problem Resolution process

Process ID	Procedure or Decision	Description	Role
SO 4.3.1	Attempt to identify permanent fix	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. 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.	Problem Analyst
SO 4.3.2	Create Known Error	If needed, create a known error record from the problem record for reference and to contribute to the known error knowledge base.	Problem Analyst
SO 4.3.3	Fix found?	If a permanent fix is identified, it is documented. If a permanent fix is not identified, it is verified for closure or deferral.	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	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. If the problem is canceled, the workflow moves to SO 4.3.7.	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
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

Problem Resolution process, continued

Process ID	Procedure or Decision	Description	Role
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
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.	Problem Analyst

Problem Resolution process, continued

Process ID	Procedure or Decision	Description	Role
		If the error is corrected, the workflow moves to SO 4.3.27.	
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	Update known error with resolution and close known error	The Problem Analyst updates the related open known error record with the problem resolution, and then closes the known error.	Problem Analyst
SO 4.3.29	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.

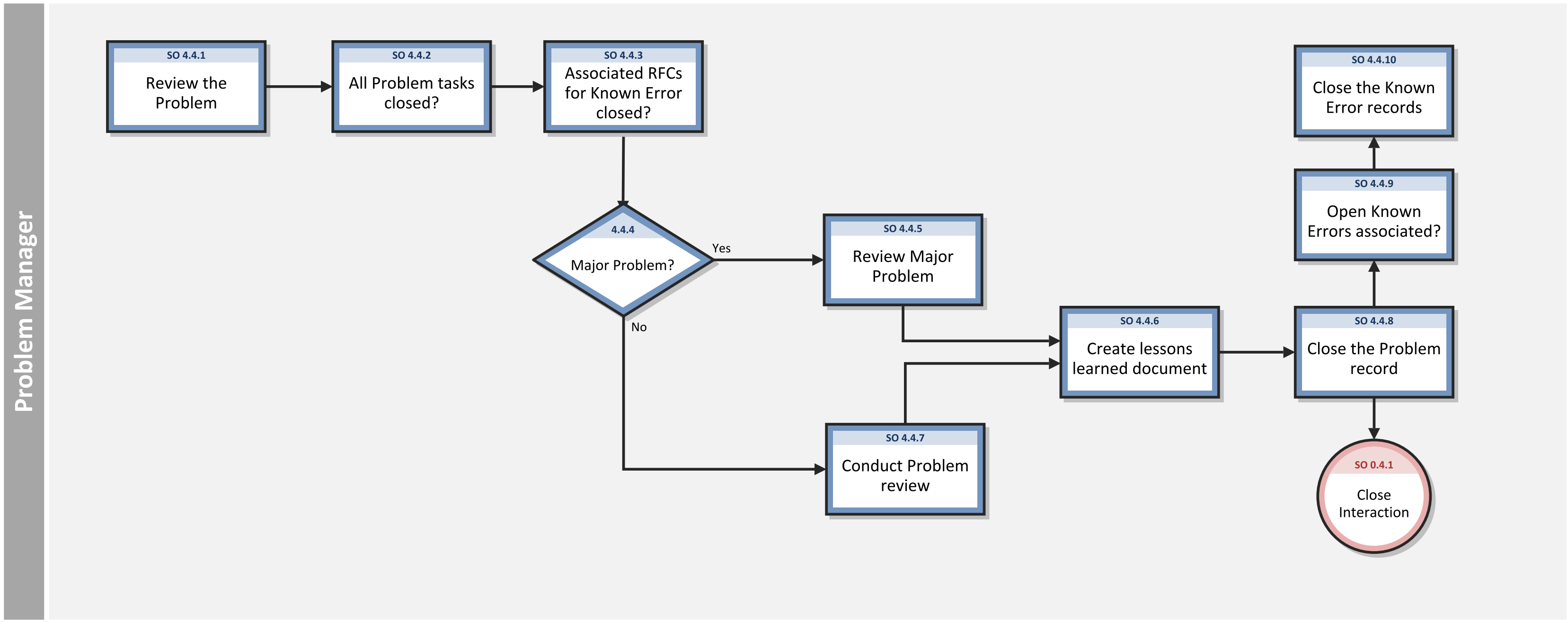
Problem reviews typically include the following elements:

- 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 4.4.5	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: • 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
SO 4.4.6	Create lessons	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	Problem Manager

Problem Review and Closure process, continued

Process ID	Procedure or Decision	Description	Role
	learned document	Process, if required.	
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
SO 4.4.9	Open Known Errors associated?	If there is an open known error associated with the problem, choose whether to close the known error as well as closing the problem.	Problem Manager
SO 4.4.10	Close the Known Error records	The Problem Manager closes the associated known error.	Problem Manager

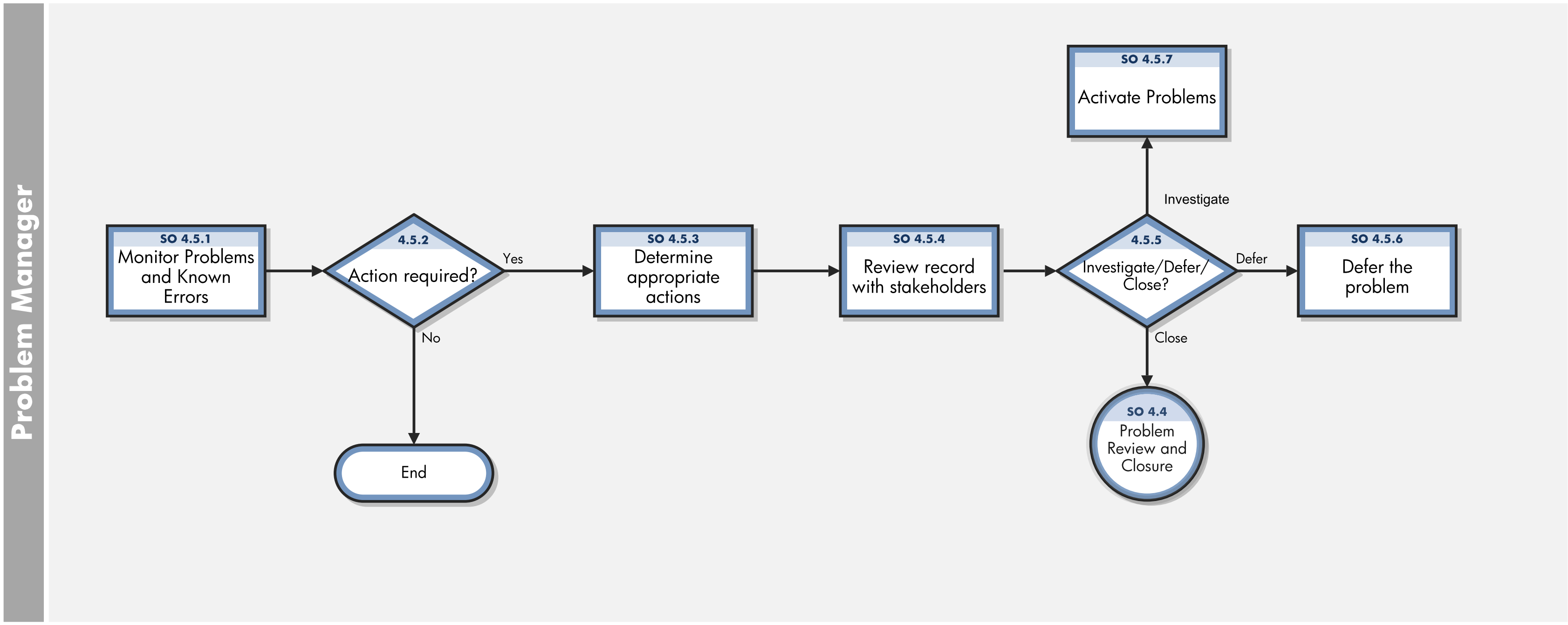
Problem and Known Error Monitoring (process SO 4.5)

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

HP Service Manager tracks individual problems and their associated known error activities. The Problem Manager evaluates the progress of those activities against the plans and associated budget. In the event that 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 and Known Errors	The Problem Manager reviews the problem and known error records periodically, and compiles a list or report of the problem records for review. This list or report includes the following items: • 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) The review may also be triggered by new releases or by changes being implemented. 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.	Problem Manager
SO 4.5.2	Action required?	If any action is required, it is performed. If no action is required, the monitoring process continues.	Problem Manager
SO 4.5.3	Determine appropriate actions	The Problem Manager identifies the appropriate action for the record. Possible actions include the following: • 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	The actions for the records are reviewed with the stakeholders.	Problem Manager
SO 4.5.5	Investigate/Defer/Close?	Determine whether the problem is still relevant. If a deferred problem record needs to be worked on, it is activated. If the problem is not relevant, the problem record is checked for closure and deferring.	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 10: 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.

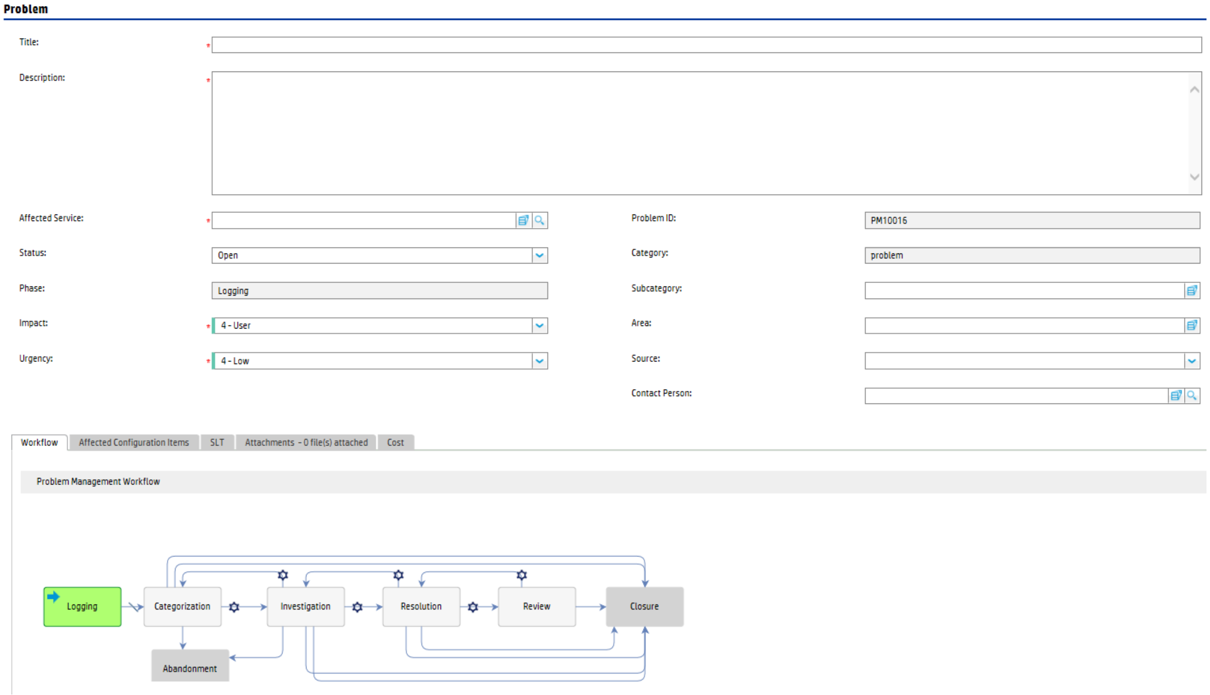
This section includes the following topics:

- "Problem form for problems opened from an incident" below
- "Problem form details" on page 148

Problem form for problems opened from an incident

After a problem is opened from an incident, the problem enters the Logging phase.

The following screenshot illustrates a new problem form:



Problem

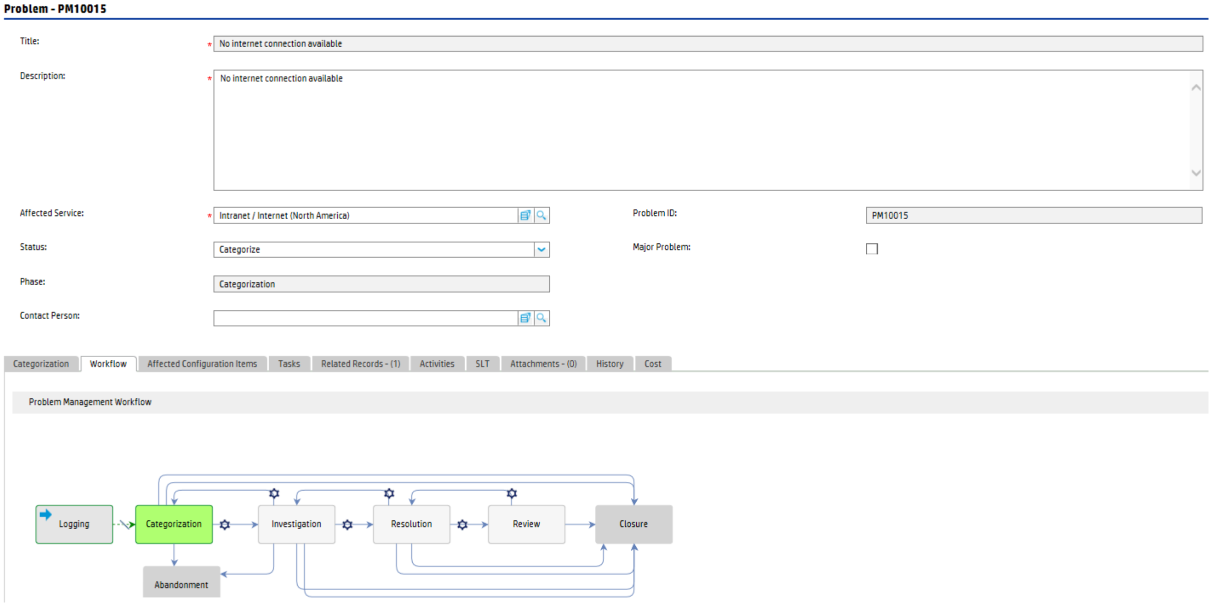
Title: *

Description: *

Affected Service: *		Problem ID:	PM10016
Status:	Open	Category:	problem
Phase:	Logging	Subcategory:	
Impact: *	4 - User	Area:	
Urgency: *	4 - Low	Source:	
		Contact Person:	

Workflow
Affected Configuration Items
SLT
Attachments - 0 file(s) attached
Cost
Problem Management Workflow
Logging
Categorization
Investigation
Resolution
Review
Closure
Abandonment

After you save the new problem form, the problem moves to the Problem Categorization phase. The Problem Manager categorizes and prioritizes problems. The following screenshot illustrates this change:



Problem - PM10015

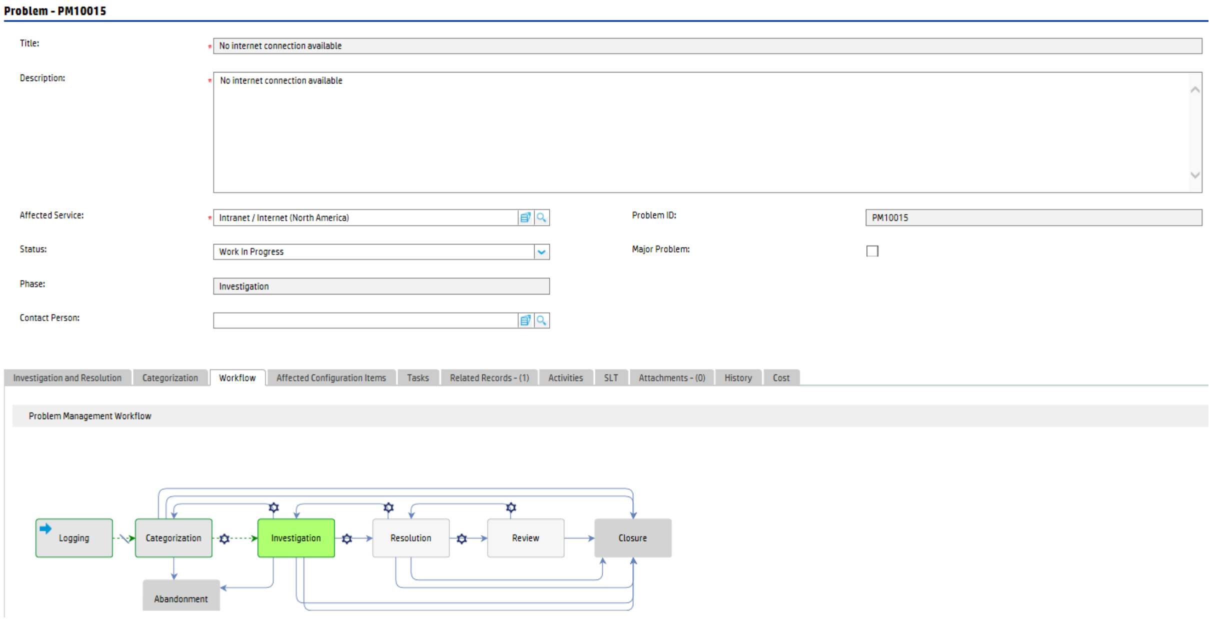
Title: * No internet connection available

Description: * No internet connection available

Affected Service: *	Intranet / Internet (North America)	Problem ID:	PM10015
Status:	Categorize	Major Problem:	□
Phase:	Categorization		
Contact Person:			

The Problem Analyst uses the problem investigation form to diagnoses the root cause of the problem and proposes solution.

The following screenshot illustrates a problem investigation form:

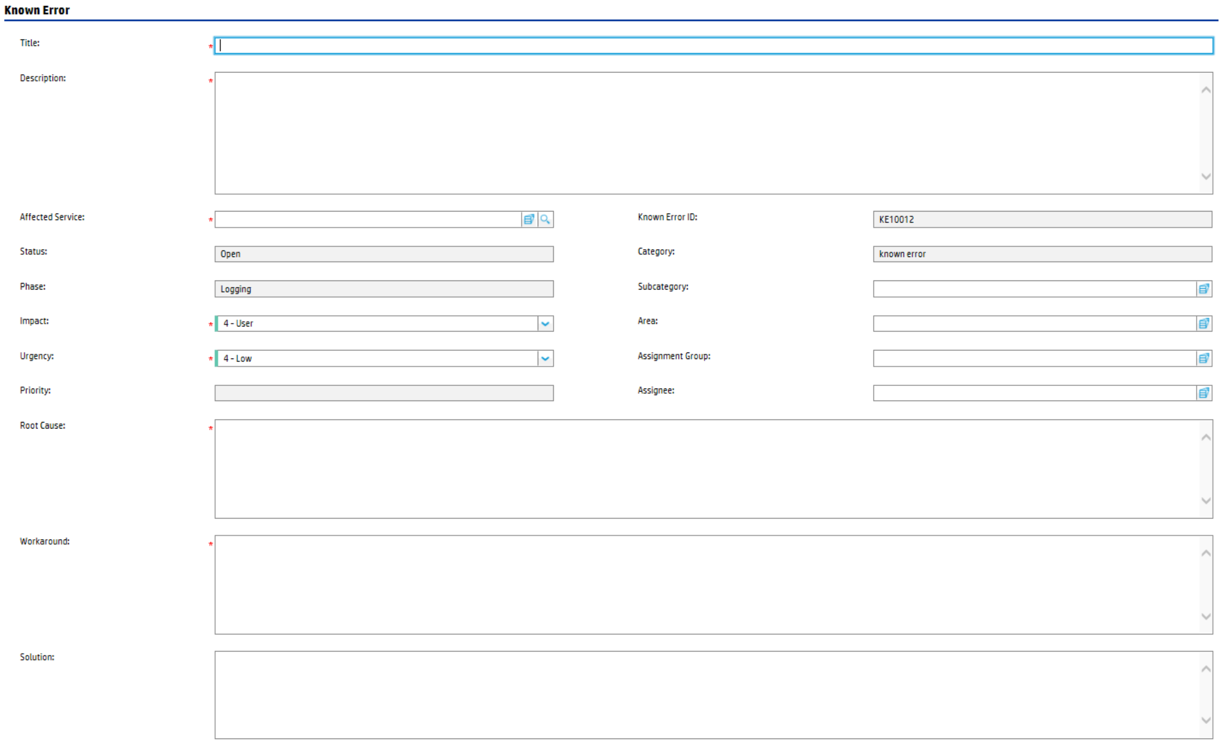


Problem - PM10015

Title:	* No internet connection available		
Description:	* No internet connection available		
Affected Service:	* Intranet / Internet (North America)	Problem ID:	PM10015
Status:	Work In Progress	Major Problem:	□
Phase:	Investigation		
Contact Person:			

The Problem Coordinator uses the form to create known error records once the root cause and workaround of the problem has been found.

The following screenshot illustrates an open known error form:

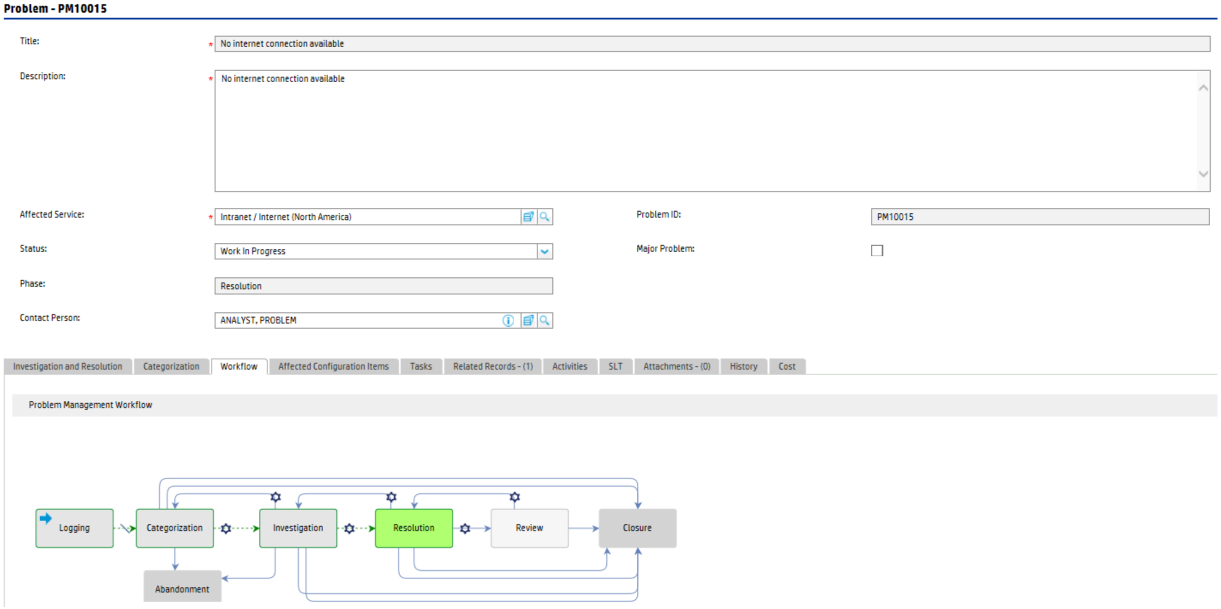


Known Error

Title:	*		
Description:	*		
Affected Service:	*	Known Error ID:	KE10012
Status:	Open	Category:	known error
Phase:	Logging	Subcategory:	
Impact:	* 4 - User	Area:	
Urgency:	* 4 - Low	Assignment Group:	
Priority:		Assignee:	
Root Cause:	*		
Workaround:	*		
Solution:			

The Problem Analyst uses the problem resolution form to implement the proposes solution to resolve the problems.

The following screenshot illustrates a problem resolution form:

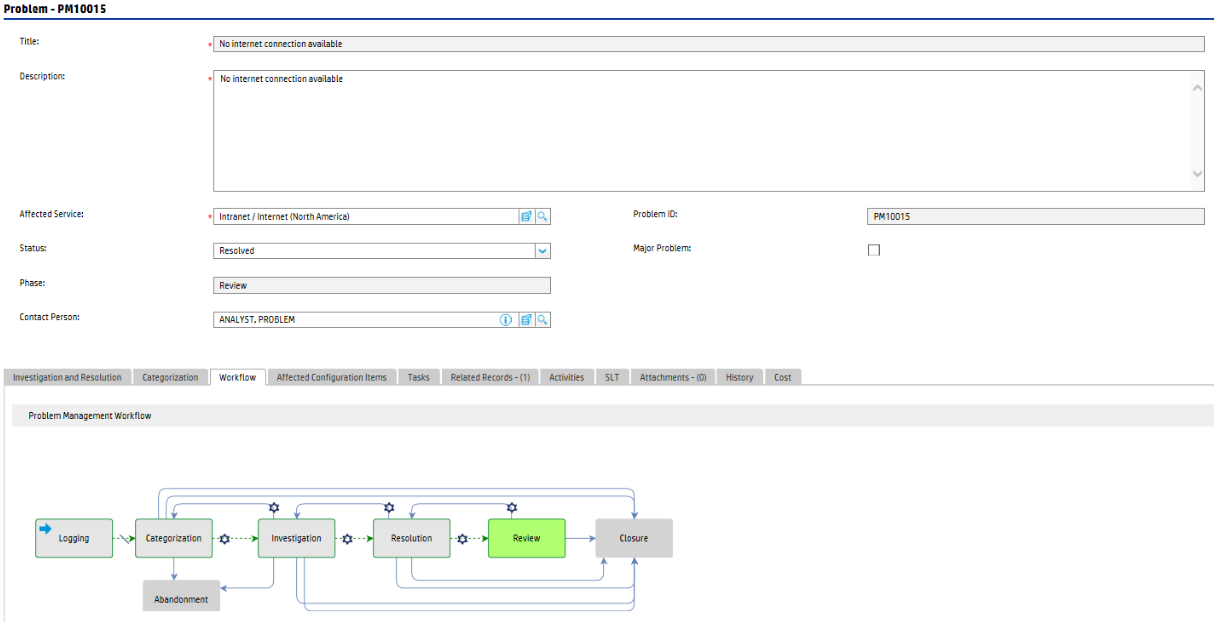


Problem - PM10015

Title:	* No internet connection available		
Description:	* No internet connection available		
Affected Service:	* Intranet / Internet (North America)	Problem ID:	PM10015
Status:	Work In Progress	Major Problem:	□
Phase:	Resolution		
Contact Person:	ANALYST, PROBLEM		

The Problem Manager uses the problem review form to conduct problem reviews.

The following screenshot illustrates a problem reviewform:



Problem - PM10015

Title:	* No internet connection available		
Description:	* No internet connection available		
Affected Service:	* Intranet / Internet (North America)	Problem ID:	PM10015
Status:	Resolved	Major Problem:	□
Phase:	Review		
Contact Person:	ANALYST, PROBLEM		

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	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. This is a required field.
Description	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. This is a required field.
Affected Service	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. For more information about this field, see the "Affected service" section of the table in "Service Desk Interaction Management form details" on page 42. This is a required field.
Phase	This is a system-generated field. The following phases are available out-of-box: • Problem Logging • Problem Categorization • Problem Investigation • Problem Resolution • Problem Review • Problem Closure • Problem Abandonment
Status	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). The following statuses are available out-of-box: • Open — The problem has been opened, but it is not currently being worked on.

Problem form details, continued

Label	Description
	- 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).
Category	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. 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.
Subcategory	The second level of categorization. This field is pre-populated with data from an escalated incident. Service Manager displays different lists of subcategories, depending on the category that you selected. The subcategories are defined on a category.
Area	The third level of classification, mainly used for reporting purposes. This field is pre-populated with data from an escalated incident. Service Manager displays different lists of areas, depending on the category and subcategory that you selected. The areas are defined on a subcategory.
Impact	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. The following impacts are available out-of-box: - 1 - Enterprise - 2 - Site/Dept - 3 - Multiple Users

Problem form details, continued

Label	Description
	- 4 - User The out-of-box data is the same as Interaction Management and Incident Management.
Urgency	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 42.
Major Problem	If selected (set to true), it indicates the problem is a major problem, then the Problem Manager needs to specified and notified.
Major Problem Review section	This section is only visible when Major Problem is selected. Review details for this major problem can be documented under this section.
Source	The source from where the Problem is reported. Below sources are available out-of-box: 1. User 2. Group 3. Event 4. Incident
Contact Person	This field is pre-populated with data from the interaction or incident when the problem is opened from an interaction or incident. It specified the contact person for the reported problem.
Categorization > Priority	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.
Categorization > Assignment Group	The group that is assigned to work on the problem. For more information about this field, see "Incident Management form details" on page 96. The out-of-box data consists of default assignment groups for use as examples of types of assignment groups. **Tip:** You may want to change the sample assignment groups to meet your own needs. The following assignment groups are available out-of-box: - Application

Problem form details, continued

Label	Description
	• 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 This is a required field when status starts from Assign and phase starts from Categorization.
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.

Problem form details, continued

Label	Description
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 theAffected Configuration Items section.The affected CI count is calculated based on the Assessment section in the Affected CIs table.
Tasks section	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: • Task ID • Status • Phase • Priority • Title
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: • Related Incidents • Caused Changes • Solved By Changes • Related Problems • Related Known Errors
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	Displays information on all the records that are related to this problem. The data displayed includes the following information:

Problem form details, continued

Label	Description
section > All Related Records table	• 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.
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 SLT Target date. The expected problem resolution date is the date when you plan to close the record. This should be done before the SLT 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 SLT. 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	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

Problem form details, continued

Label	Description
Resolution section > Solution Identified Date	"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.
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.
Cost section	The user can add cost details of parts and labor for this incident handling. For more information about this field, see "Incident Management form details" on page 96.

Chapter 11: Change Management Overview

The HP Service Manager Change Management application, referred to as Change Management throughout this chapter, supports the Change Management process. It controls the process to request, manage, approve, and control changes that modify your organization’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 Fulfillment

Change Management and Request Fulfillment are separate processes, but they are closely related. Change Management handles any change to your business that modifies or disrupts the current state of that environment. Usually these modifications or disruptions affect multiple users or business units. Request Fulfillment handles common user requests for products and services. These requests usually affect only the person making the request, or a subordinate group of employees.

- Change Management
  - Manages changes (implementations) that modify a business environment.
  - Affects many users.
  - Scope is often large, including large groups or multiple business units.
- Request Fulfillment
  - Handles common requests for products and services.
  - Affects a small or limited number of users.
  - Scope is limited.

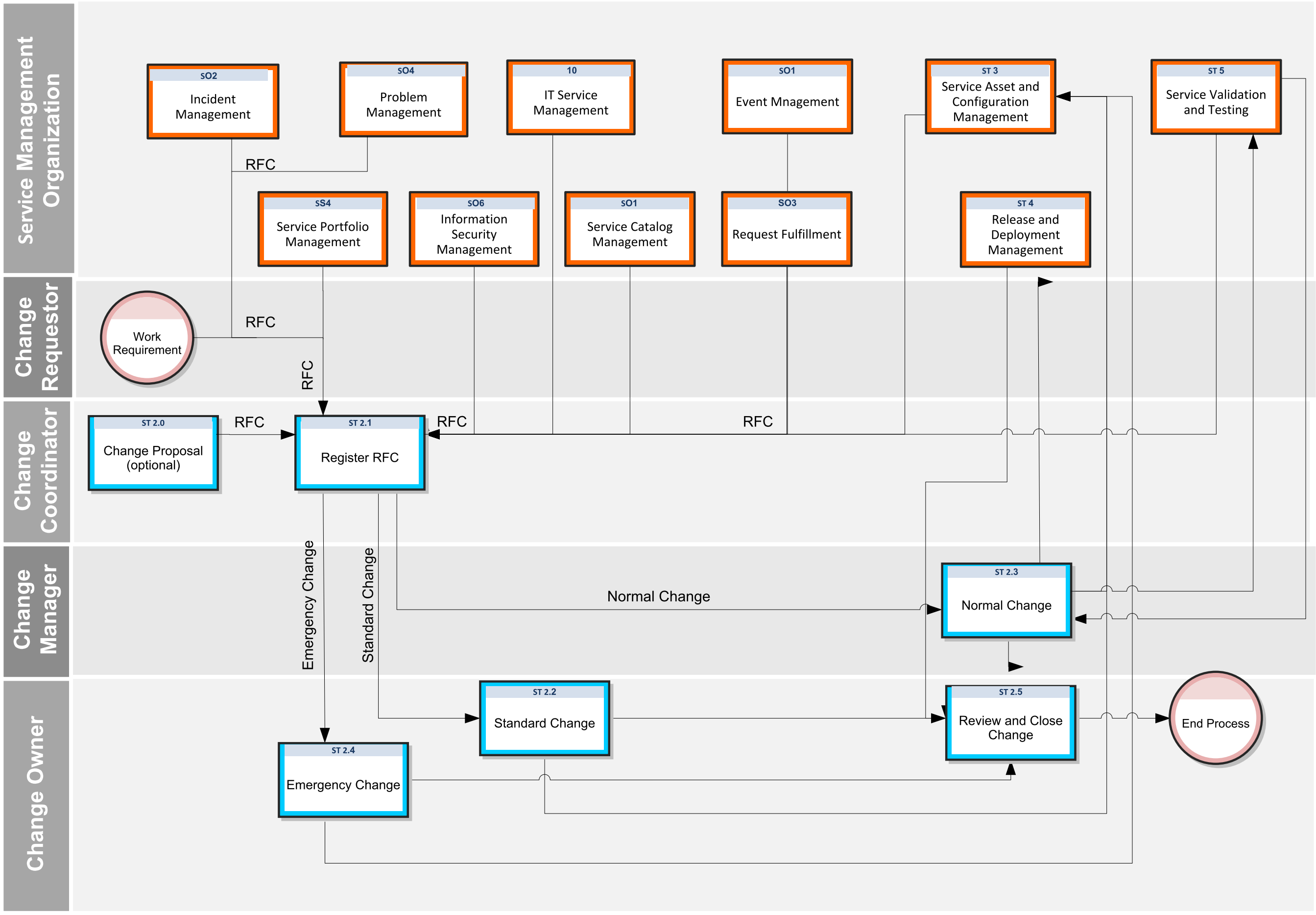
Change Management process overview

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 170.



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 best practice process flows shipped with the Process Designer framework introduce four processes: Change Proposal, Standard, Normal and Emergency changes, which correspond to the "Change Proposal", "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. They are added to any existing categories including any previous out-of-box 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.

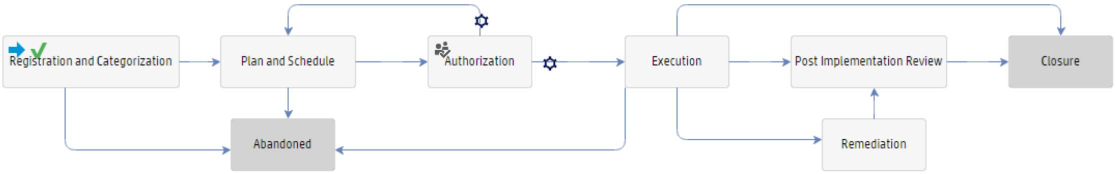
Change Management categories

Category	Description
Change Proposal	A Change Proposal is a high-level description of the suggestion or request for a new or changed service, in order to ensure that potential conflicts for resources or other issues are identified. For example, major changes that involve significant cost, risk or organizational impact are usually initiated by a change proposal.
Emergency Change	Emergency changes are the change processes to be applied in the production environment during emergency situations like service outage.
Normal Change	A Normal Change is a change that is categorized, prioritized, planned and that follows all approvals before deployment. Normal Changes can be further categorized as Major RFC, Significant RFC, and Minor RFC.
Standard Change	A Standard Change is a pre-authorized 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.

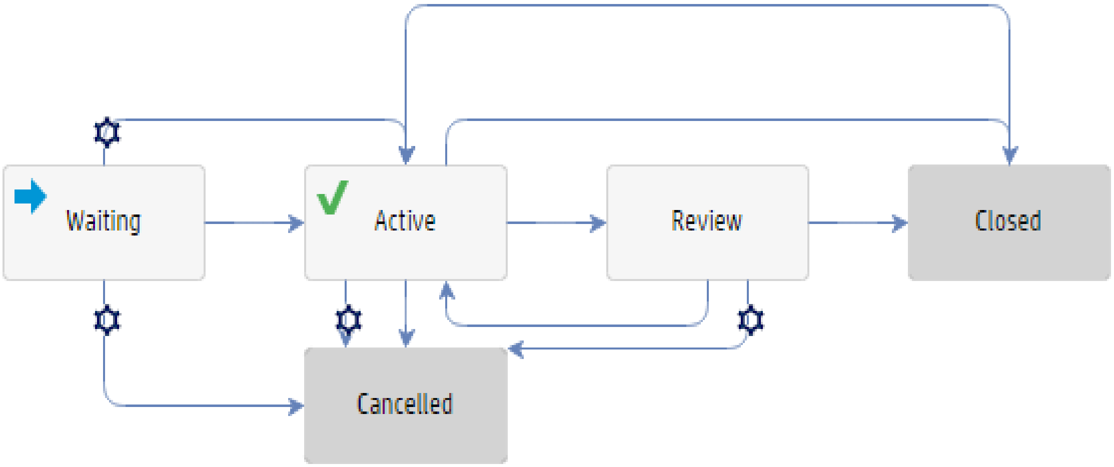
Change Management tasks include:

- 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 Desinger.



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. Log on 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

Value	Status
1	Ready
2	Assigned
3	In Progress
4	Blocked
20	Completed
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	• 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	• 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.

Change Management user roles, continued

Role	Responsibilities
	• If a change implementation fails, the coordinator activates a back-out plan to return the system to its original state.
Change Owner	• 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	• 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	• 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.
Technical Change Advisory Board (TCAB)	• Responsible for analyzing and reviewing the risk and impact of change request.

Change Management user roles, continued

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

Key performance indicators for Change Management

The Key Performance Indicators (KPIs) in 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.
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 2011 and COBIT 4.1 KPIs are included in the following sections.

ITIL 2011 Key Performance Indicators

The following are ITIL 2011 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			
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	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
	Requirements						
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
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

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 2.4.8	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
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 12: 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 Fulfillment.

Change Management automates the approval process and eliminates the need for memos, E-mail, and phone calls.

Note: The 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. 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.

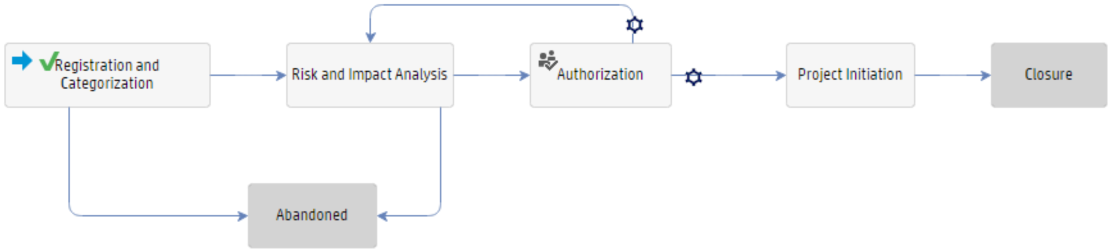
- Change Proposal (process ST 2.0)
- Register RFC (process ST 2.1)
- Standard Change (process ST 2.2)
- Normal Change (process ST 2.3)
- Emergency Change (process ST 2.4)
- Review and Close Change (process ST 2.5)

Change Proposal (process ST 2.0)

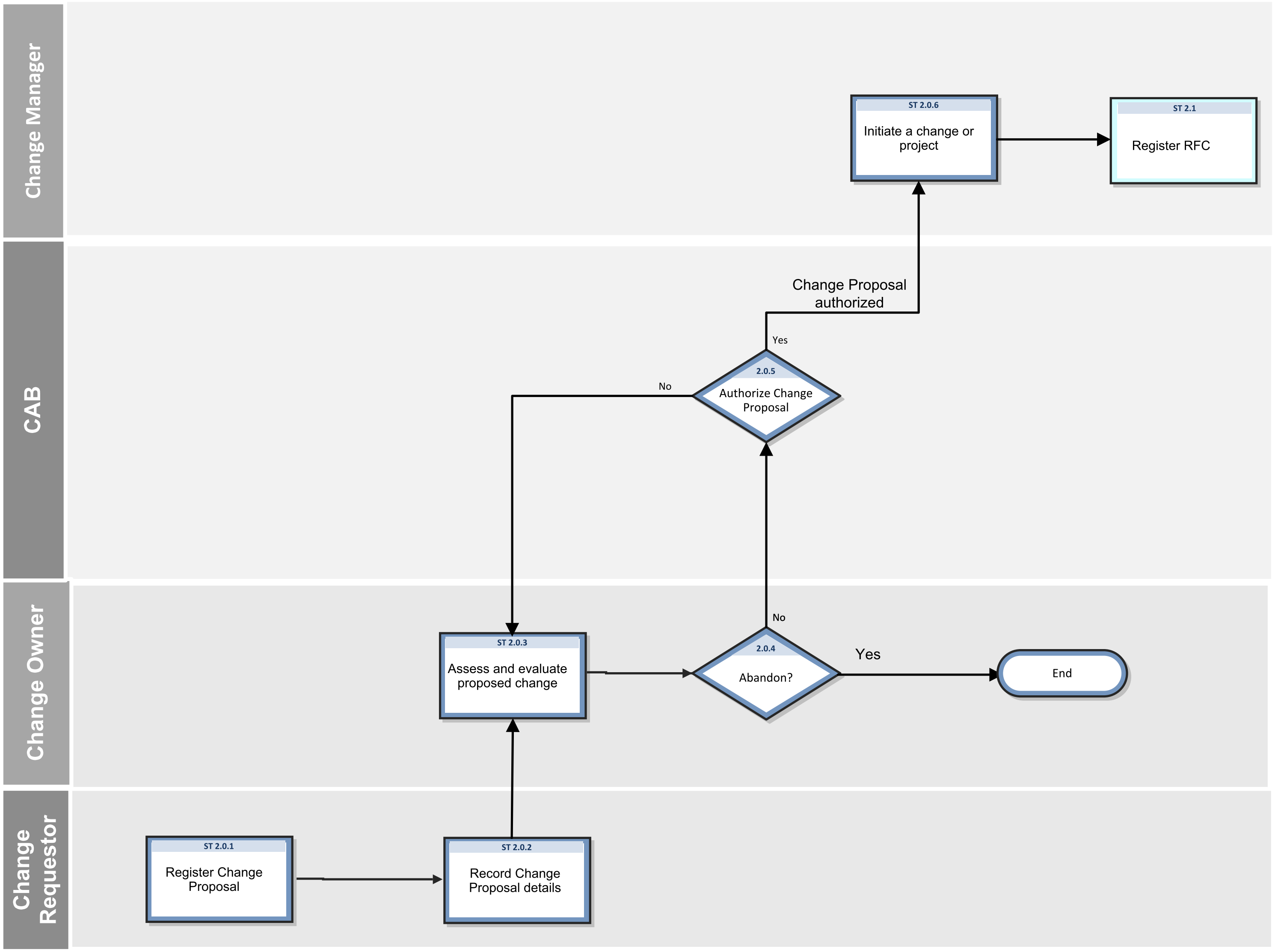
Change proposals are submitted to change management before chartering new or changed services in order to ensure that potential conflicts for resources or other issues are identified. Authorization of the change proposal does not authorize implementation of the change but simply allows the service to be chartered so that service design activities can commence.

A change proposal is used to communicate a high-level description of a change. This change proposal is normally created by the service portfolio management process and is passed to change management for authorization. In some organizations, change proposals may be created by a programme management office or by individual projects.

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



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


Change Manager
CAB
Change Owner
Change Requestor
ST 2.0.6
Initiate a change or project
ST 2.1
Register RFC
Change Proposal authorized
Yes
2.0.5
Authorize Change Proposal
No
No
ST 2.0.3
Assess and evaluate proposed change
2.0.4
Abandon?
Yes
End
ST 2.0.1
Register Change Proposal
ST 2.0.2
Record Change Proposal details

Change Proposal (process ST 2.0)

Process ID	Procedure or Decision	Description	Role
ST 2.0.1	Register Change proposal	The change requester logs a change proposal with a high-level description of the proposed change.	Change Requester
ST 2.0.2	Records Change proposal details	The change owner records details of the change proposal. The change proposal should include the following items: • A high-level description of the new, changed or retired service, including business outcomes to be supported, and utility and warranty to be provided • A full business case including risks, issues and alternatives, as well as budget and financial expectations • An outline schedule for design and implementation of the change	Change Requester
ST 2.0.3	Assess and evaluate proposed Change	The change owner assesses and evaluates the change proposal, including risks, issues and alternatives, as well as budget and financial expectations.	Change Owner
ST 2.0.4	Abandon?	The change owner decides whether to abandon the proposal or not.	Change Owner
ST 2.0.5	Authorize Change proposal	CAB reviews the change proposal and the current change schedule, identifies any potential conflicts or issues and responds to the change proposal by either authorizing it or documenting the issues that need to be resolved.	CAB
ST 2.0.6	Initiate a change or project	After the new or changed service is chartered, RFCs will be used in the normal way to request authorization for specific changes. These RFCs will be associated with the change proposal so that change management has a view of the overall strategic intent and can prioritize and review these RFCs appropriately.	Change Manager

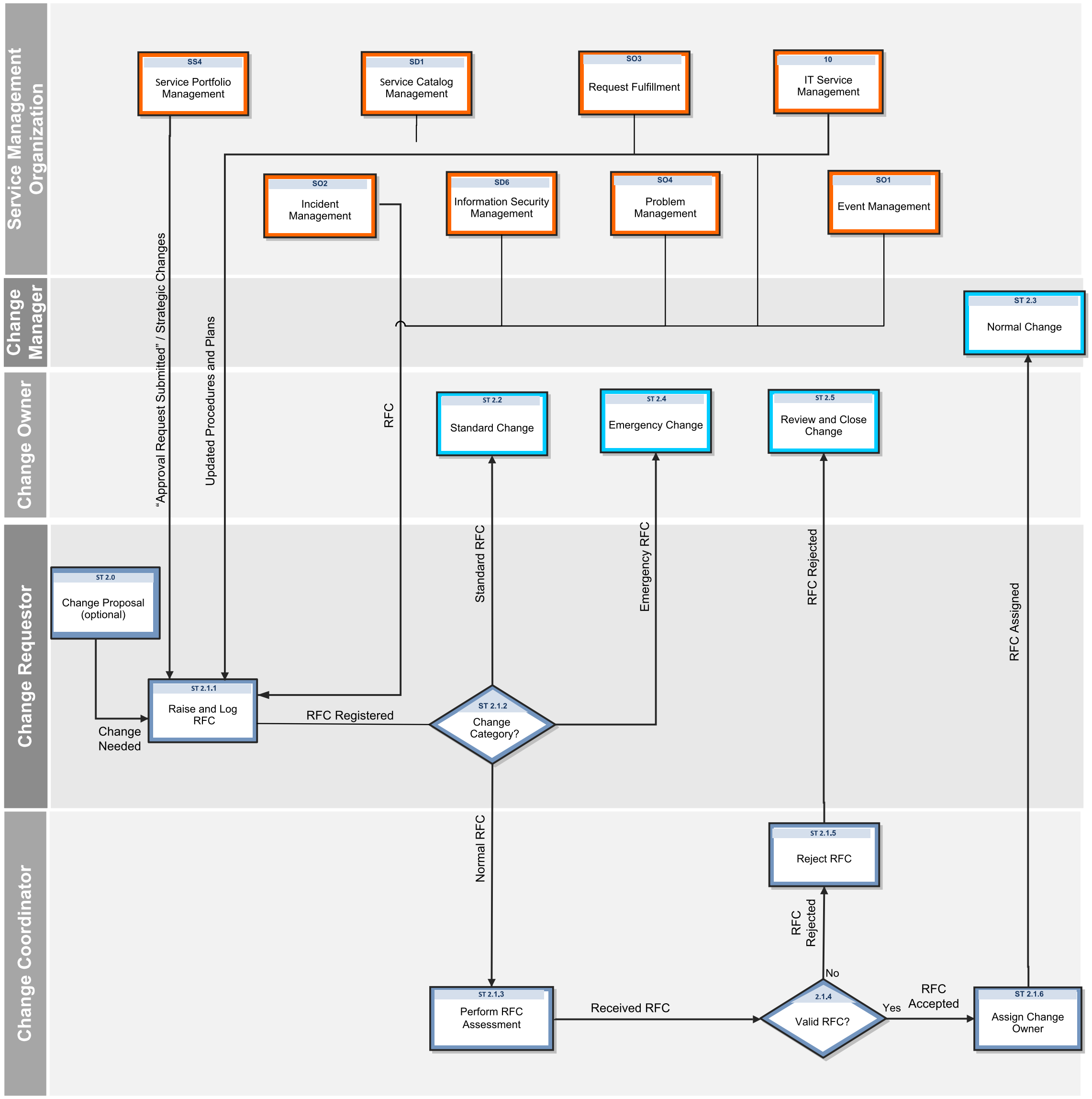
Register RFC (process ST 2.1)

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.


Service Management Organization
Change Manager
Change Owner
Change Requestor
Change Coordinator
SS4
Service Portfolio Management
SD1
Service Catalog Management
SO3
Request Fulfillment
10
IT Service Management
SO2
Incident Management
SD6
Information Security Management
SO4
Problem Management
SO1
Event Management
ST 2.3
Normal Change
"Approval Request Submitted" / Strategic Changes
Updated Procedures and Plans
RFC
ST 2.2
Standard Change
ST 2.4
Emergency Change
ST 2.5
Review and Close Change
Standard RFC
Emergency RFC
RFC Rejected
RFC Assigned
ST 2.0
Change Proposal (optional)
ST 2.1.1
Raise and Log RFC
Change Needed
RFC Registered
ST 2.1.2
Change Category?
Normal RFC
ST 2.1.5
Reject RFC
RFC Rejected
No
ST 2.1.3
Perform RFC Assessment
Received RFC
2.1.4
Valid RFC?
Yes
RFC Accepted
ST 2.1.6
Assign Change Owner

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: • The RFC is impractical • The RFC is a duplicate **Note:** The activities of logging and categorizing an RFC may be delegated to a Change Coordinator if desired.	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

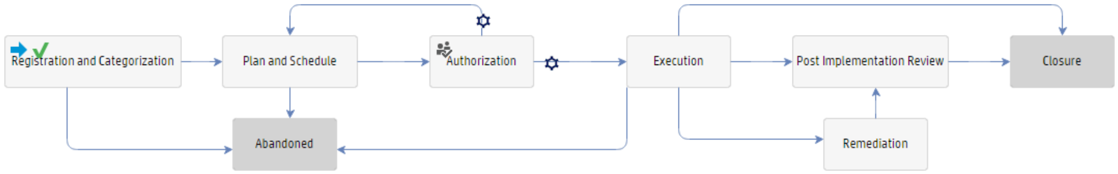
Standard Change (process ST 2.2)

A Standard Change is a pre-authorized 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.

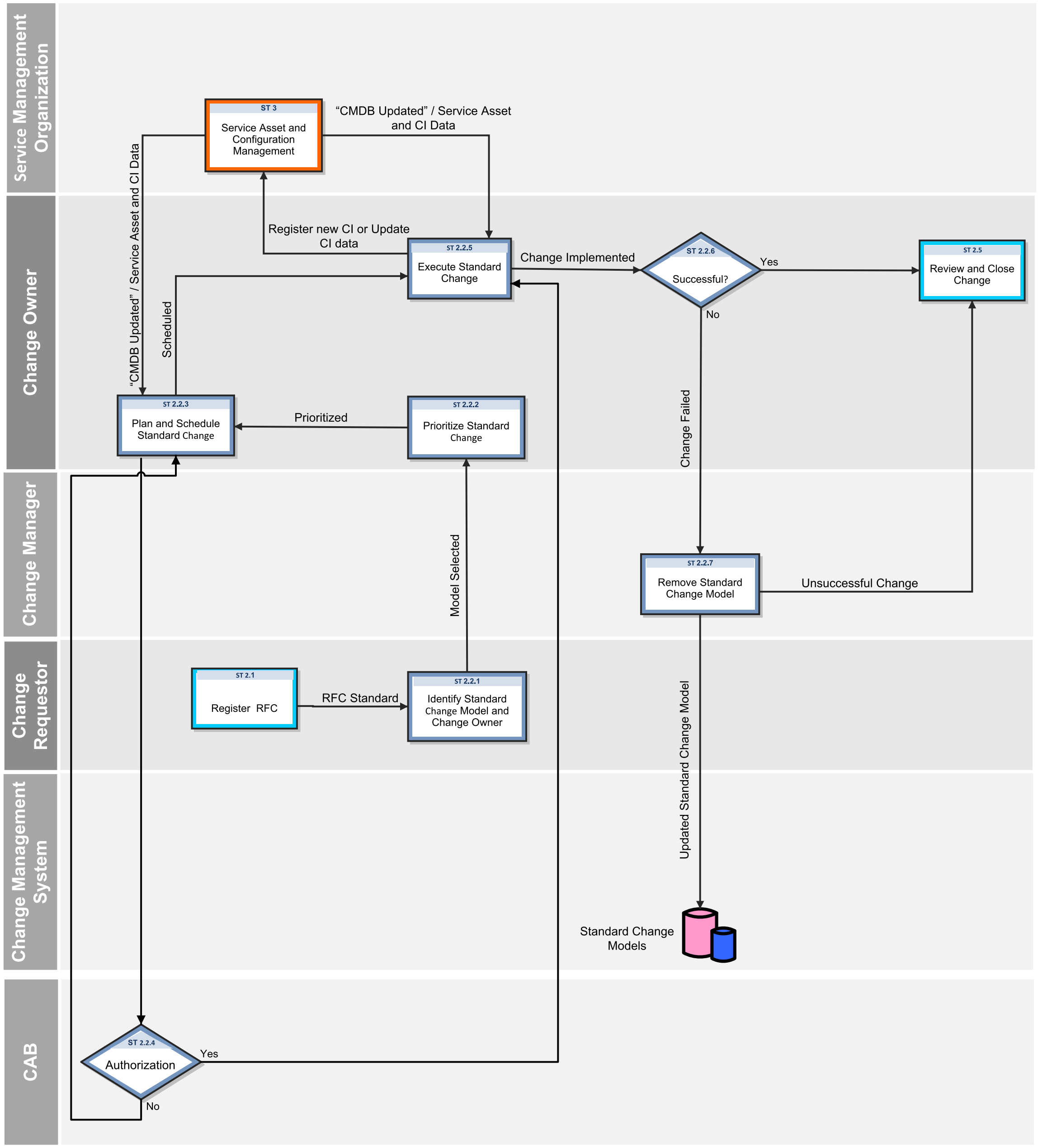
For an activity to be accepted as a Standard Change, the following requirements must be met:

- 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 Requester

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



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


Service Management Organization
Change Owner
Change Manager
Change Requestor
Change Management System
CAB
ST 3
Service Asset and Configuration Management
"CMDB Updated" / Service Asset and CI Data
"CMDB Updated" / Service Asset and CI Data
Register new CI or Update CI data
ST 2.2.5
Execute Standard Change
Change Implemented
ST 2.2.6
Successful?
Yes
No
ST 2.5
Review and Close Change
Scheduled
ST 2.2.3
Plan and Schedule Standard Change
Prioritized
ST 2.2.2
Prioritize Standard Change
Change Failed
Model Selected
ST 2.2.7
Remove Standard Change Model
Unsuccessful Change
ST 2.1
Register RFC
RFC Standard
ST 2.2.1
Identify Standard Change Model and Change Owner
Updated Standard Change Model
Standard Change Models
ST 2.2.4
Authorization
Yes
No

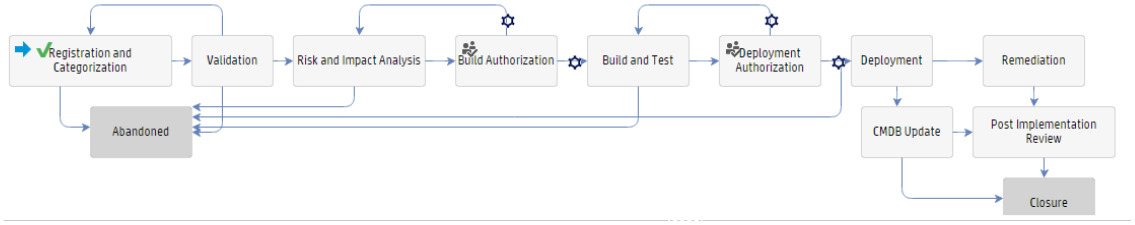
Standard Change process

Process ID	Procedure or Decision	Description	Role
ST 2.1	Register RFC	The change requester logs an RFC and reviews the RFCs for completeness and accuracy.	Change Requester
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 Requester
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	Authorize Plan and Schedule	The Change Advisory Board (CAB) reviews and authorizes the resource plan and change schedule. If not authorized, the change returns to process ST 2.2.3.	CAB
ST 2.2.5	Execute Standard Change	The Change Owner executes the Standard Change. The CMDB is updated according to the changes performed.	Change Owner
ST 2.2.6	Successful?	The Change Owner checks whether the Change is successful.	Change Owner
ST 2.2.7	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

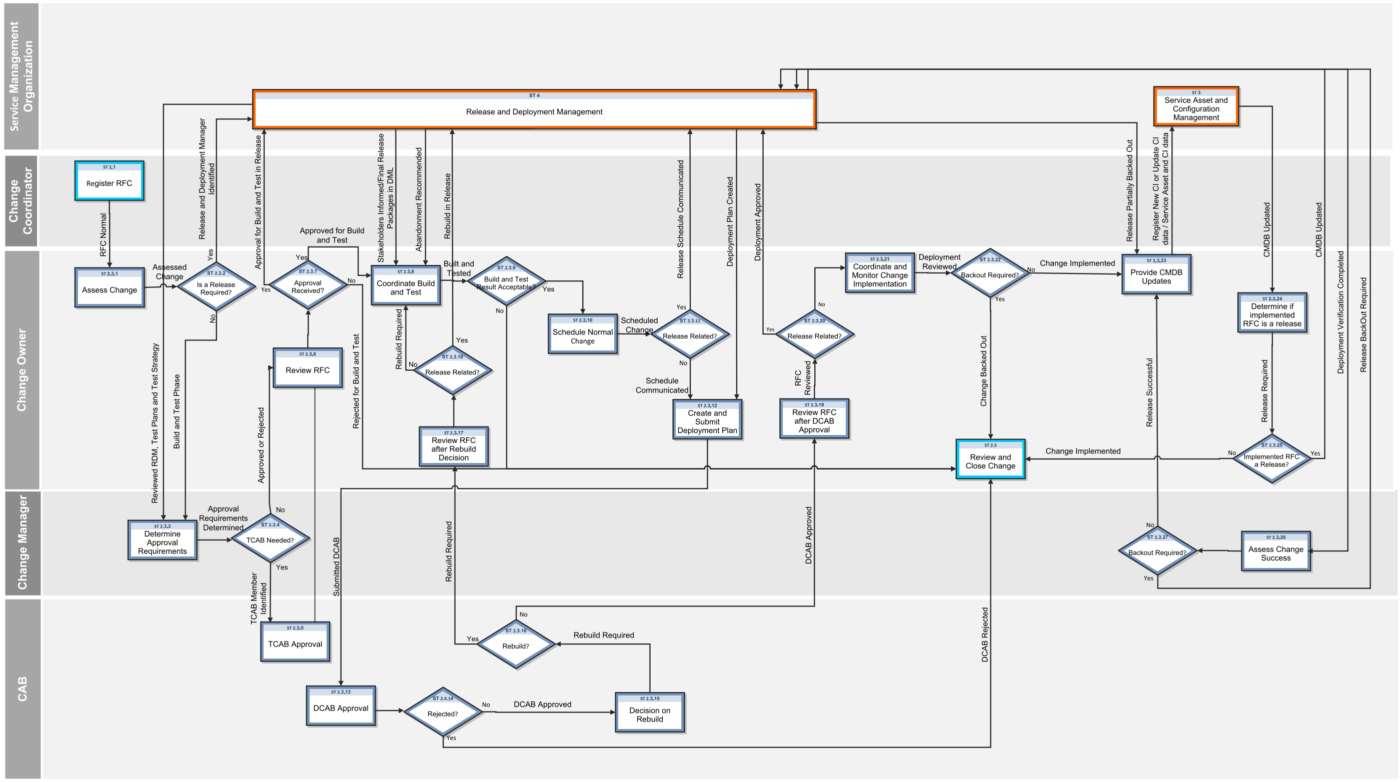
Normal Change (process ST 2.3)

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. A Normal Change can be further categorized as Major, Significant, and Minor. All Major, Significant, and Minor changes go through the same workflow except that, for a Normal Major RFC or a Normal Significant RFC the Build Authorization phase is a manual transition and the change has to be approved manually by Change Advisory Board (CAB) members. In a Normal Minor RFC the Build Authorization phase is auto approved. The Build Authorization phase is optional in a Minor RFC but it is still configured in the out-of-box system. 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

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
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	Build Authorization Needed?	If Build Authorization is not needed, the Change Manager determines whether the change should be approved or rejected. If Build Authorization is needed, members are identified and change is submitted for approval.	Change Manager
ST 2.3.5	Build Authorization	Change Manager works with CAB 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
ST 2.3.8	Coordinate Build and Test	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. 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. The Change Owner coordinates between the experts within Change process for building and testing activities. The change is built and tested thoroughly and validated.	Change Owner
ST 2.3.9	Build and Test	If the Build and Test result is acceptable, deployment is scheduled; else the RFC is sent for closure.	Change

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
	Result Acceptable?		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 CAB approval. The same is also received from RDM and is sent for CAB's review.	Change Owner
ST 2.3.13	Deployment Authorization	CAB reviews the Build and Test results and approves / abandons / rejects as deemed fit. If the Build and Test results are approved, CAB reviews and updates the implementation schedule and authorizes the Normal Change implementation to commence.	CAB
ST 2.3.14	Rejected?	If the deployment plan is rejected, the change moves back to Build and Test.	CAB
ST 2.3.15	Decision on Rebuild	If CAB decides on rebuilding, the change is rebuilt and tested again.	CAB
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; if not, these are performed within the Change Management process.	Change Owner
ST 2.3.19	Review RFC after Deployment	The Change Owner reviews the RFC to go ahead with the deployment.	Change Owner

Normal Change process, continued

Process ID	Procedure or Decision	Description	Role
	Authorization		
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	Remediation 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
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	Remediation 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:

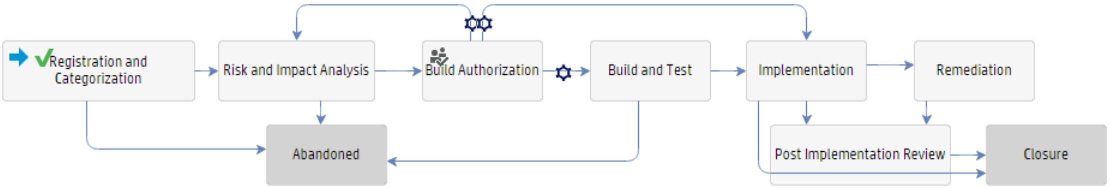
- Approval is given by the Emergency Change Approval Board (E-CAB) instead of waiting for a regular CAB meeting.
- Testing may be reduced, or in extreme cases eliminated, if doing so is considered necessary to deliver the change immediately.
- Updating of the change request and configuration data may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

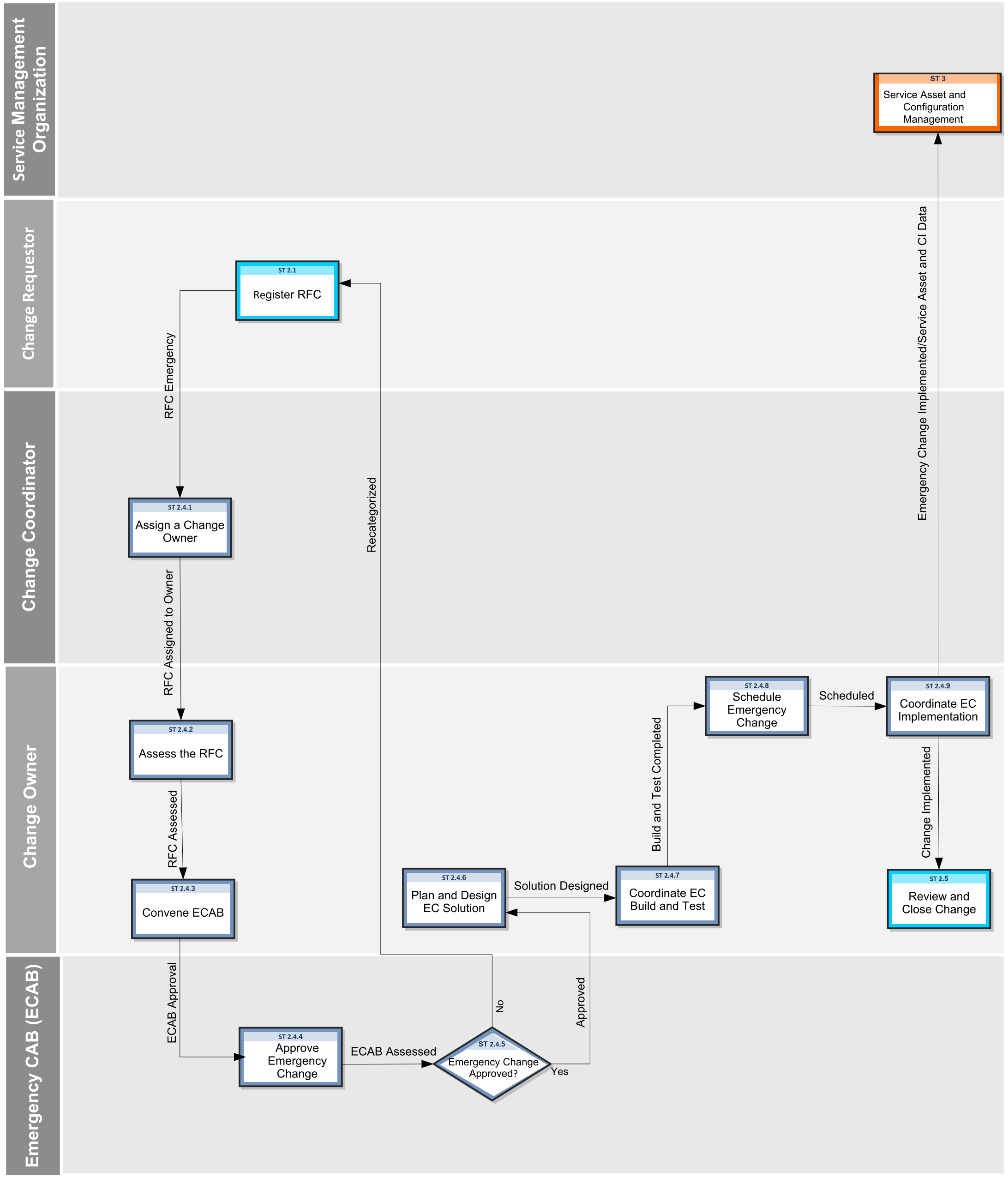
The following user roles are involved in Emergency Change Handling:

- 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.


Service Management Organization
Change Requestor
Change Coordinator
Change Owner
Emergency CAB (ECAB)
ST 3
Service Asset and Configuration Management
ST 2.1
Register RFC
RFC Emergency
ST 2.4.1
Assign a Change Owner
RFC Assigned to Owner
ST 2.4.2
Assess the RFC
RFC Assessed
ST 2.4.3
Convene ECAB
ECAB Approval
ST 2.4.4
Approve Emergency Change
ECAB Assessed
ST 2.4.5
Emergency Change Approved?
No
Yes
Recategorized
Approved
ST 2.4.6
Plan and Design EC Solution
Solution Designed
ST 2.4.7
Coordinate EC Build and Test
Build and Test Completed
ST 2.4.8
Schedule Emergency Change
Scheduled
ST 2.4.9
Coordinate EC Implementation
Emergency Change Implemented/Service Asset and CI Data
Change Implemented
ST 2.5
Review and Close Change

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 recategorized 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
ST 2.4.8	Coordinate Emergency	The Change Owner coordinates the Build and Test activities for Emergency Change.	Change Owner

Emergency Change process, continued

Process ID	Procedure or Decision	Description	Role
	Change Build and Test		
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)

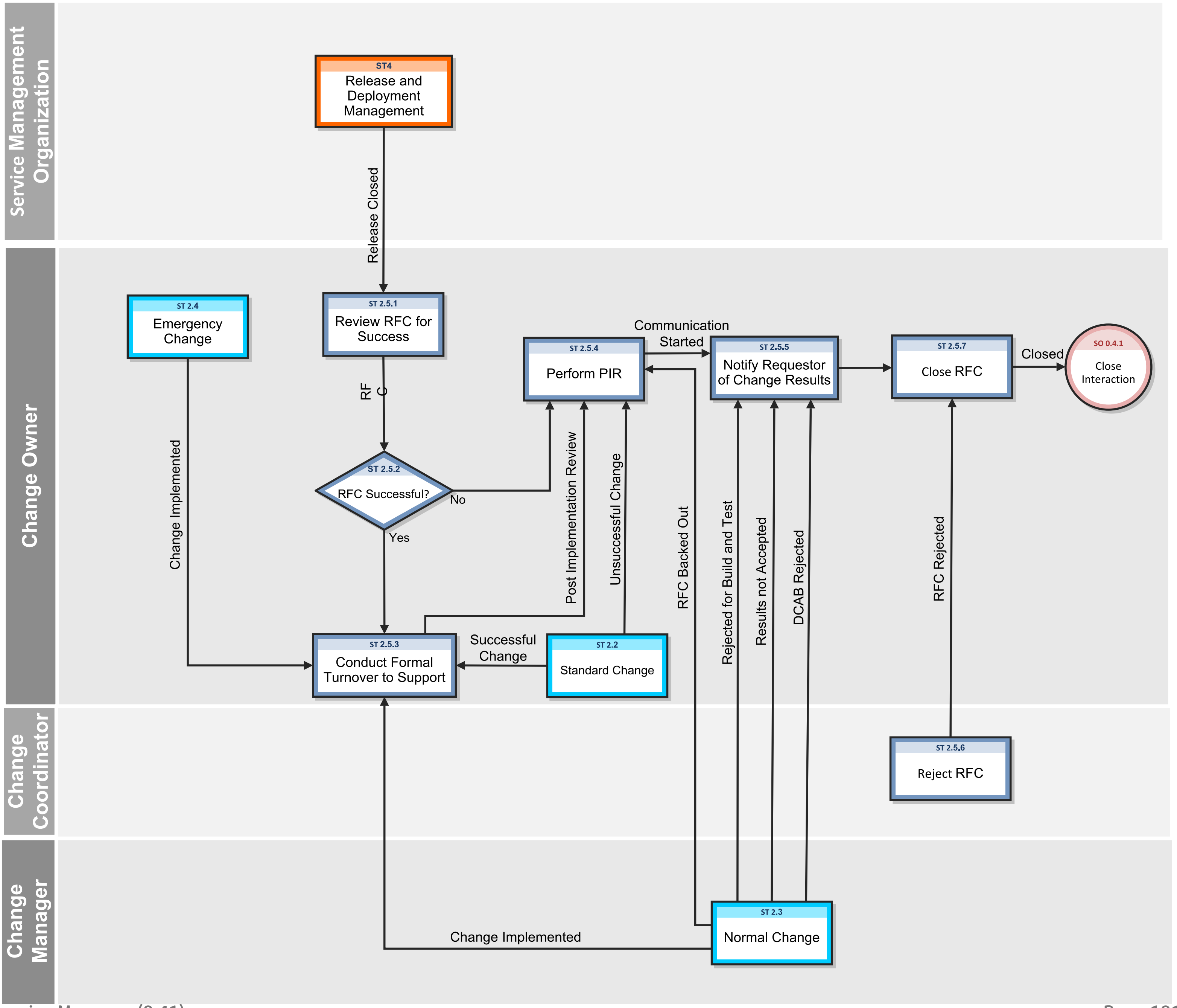
After a change is completed, the results must be reported for evaluation to those responsible for managing changes, and then presented for stakeholder agreement. This process includes the closing of related user interactions, incidents, and known errors. The Change Owner and Change Manager review the change implementation and close it if successful.

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

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

By default, an Emergency Change or a Normal Change requires PIR, while a Standard Change does not.

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


Service Management Organization
Change Owner
Change Coordinator
Change Manager
ST4
Release and Deployment Management
Release Closed
ST 2.4
Emergency Change
ST 2.5.1
Review RFC for Success
RF C
ST 2.5.2
RFC Successful?
No
Yes
Change Implemented
ST 2.5.4
Perform PIR
Communication Started
ST 2.5.5
Notify Requestor of Change Results
ST 2.5.7
Close RFC
Closed
SO 0.4.1
Close Interaction
Post Implementation Review
Unsuccessful Change
RFC Backed Out
Rejected for Build and Test
Results not Accepted
DCAB Rejected
RFC Rejected
ST 2.5.3
Conduct Formal Turnover to Support
Successful Change
ST 2.2
Standard Change
ST 2.5.6
Reject RFC
ST 2.3
Normal Change
Change Implemented

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	Reject RFC	The Change Coordinator rejects the RFC.	Change Coordinator
ST 2.5.7	Close RFC	The Change Requestor is notified of the success or failure of the change.	Change Owner

Chapter 13: Change Management Details

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

In Change Management, the Change Manager sends the change requests to the appropriate approvers and coordinates Emergency Change handling. The Change Approver and 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.

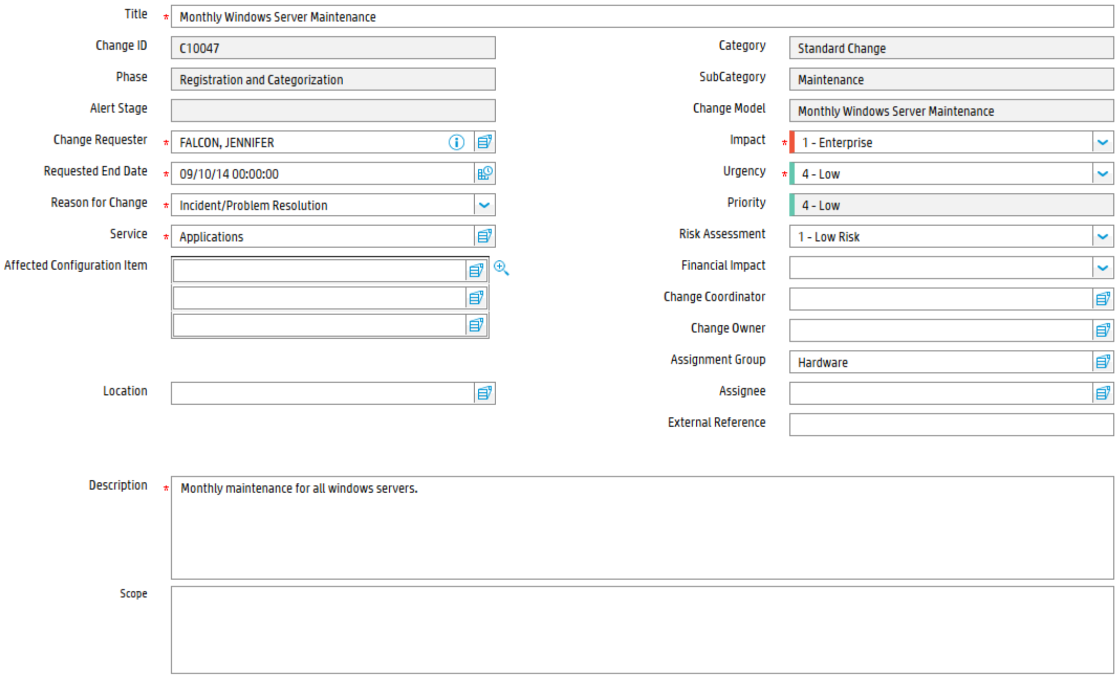
This section describes selected Change Management fields in the out-of-box Service Manager system.

Topics in this section include:

- Change Management form after escalation from a problem
- Change Management form details

Change Management form created from a problem

The following figure shows an example new change request that is created 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 195 for a list and description of the fields on this form.



Title	* Monthly Windows Server Maintenance		
Change ID	C10047	Category	Standard Change
Phase	Registration and Categorization	SubCategory	Maintenance
Alert Stage		Change Model	Monthly Windows Server Maintenance
Change Requester	* FALCON, JENNIFER	Impact	* 1 - Enterprise
Requested End Date	* 09/10/14 00:00:00	Urgency	* 4 - Low
Reason for Change	* Incident/Problem Resolution	Priority	4 - Low
Service	* Applications	Risk Assessment	1 - Low Risk
Affected Configuration Item		Financial Impact	
		Change Coordinator	
		Change Owner	
		Assignment Group	Hardware
Location		Assignee	
		External Reference	
Description	* Monthly maintenance for all windows servers.		
Scope			

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	This is a system-generated field that defines the global approval status for the change, not for a single approval. The system sets this field depending on current approvals and the approval type defined for the module. These approval statuses are available out-of-box: • Pending • Approved • Denied
Change Requester	The name of the user requesting the change. 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.
Assignment Group	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. You may want to change the sample assignment groups to meet your own needs. These assignment groups are available out-of-box: • Application • Email / Webmail

Change Management field descriptions, continued

Label	Description
	• Field Support • Hardware • Intranet / Internet Support • Network • Office Supplies • Office Support • Operating System Support • SAP Support • Service Desk • Service Manager
Change Coordinator	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.
Service	Specifies the service affected by the change. This is a system-generated field and is prepopulated when a change request is created from an interaction. This is a required field.
Affected CI	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.
Scope	Provides a detailed description of the change scope.
Category	This is a system-generated field that classifies the type of change.
Emergency Change	When checked, the system handles the change according to the emergency change process. The system adds the ECAB approval group requirement and this allows the change to skip some approvals and phases to speed up the process. Emergency changes go directly to the Prepare for Change Approval

Change Management field descriptions, continued

Label	Description
	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. There are notifications to the Change Manager every time there is an activity (open, update or closure of an emergency change).
Impact	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. These impacts are available out-of-box: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User The out-of-box data is the same as Interaction Management, Problem Management, and Incident Management. This is a required field.
Urgency	The urgency indicates how pressing the change is for the organization. The urgency and the impact are used to calculate the priority. This field functions similarly to the same field for interaction, incident, and problem tickets. For more information, see User Interaction Management form details in the Service Manager Processes and Best Practices Guide. This is a required field.
Priority	This is a system-generated field using the urgency and impact of the change. This field functions similarly to the same field for interaction, incident, and problem tickets. For additional information, see User Interaction Management form details in the Service Manager Processes Processes and Best Practices Guide.
Risk Assessment	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. These risk assessments are available out-of-box: • 0 - No Risk • 1 - Low Risk

Change Management field descriptions, continued

Label	Description
	• 2 - Some Risk • 3 - Moderate Risk • 4 - High Risk • 5 - Very High Risk After a user selects this field, the change may require additional approvals based on the risk. The approval is based on the risk number in the assessment approval record. This is a required field.
Financial Impact	Specifies a code that indicates the financial impact of the change. These financial impact codes are available out-of-box: • 1 - High • 2 - Medium • 3 - Low
Review Required	This option specifies whether post-implementation review is required or not. By default, it is set to true for Emergency and Normal changes in the Risk and Impact Analysis phase, while false for Standard changes in the Plan and Schedule phase. This field cannot be changed in subsequent phases.
Requested End Date	The system prepopulates this field if the change request is triggered from an interaction. This is the date the change initiator requests the change implementation. This is a required field if not prepopulated.
Alert Stage	This is a system-generated field that lists the current Alert Stage of this request. Change Management updates this field automatically when processing alerts against this change. Do not update it manually. The alerts are processed against a change by using the phase definition. This field is not active in an out-of-box system and must be manually enabled.
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	The date and time when the change is scheduled to end. Scheduled

Change Management field descriptions, continued

Label	Description
End	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.
Closure Code	The completion code indicates the way a change is closed. VALID VALUES • 1 - Successful • 2 - Successful (with problems) • 3 - Failed • 4 - Rejected • 5 - Withdrawn

Change Management field descriptions, continued

Label	Description
	• 6 - Cancelled
Associated CIs section > CMDB attributes need to be changed for CIs in the list Completed/Cancelled CMDB attributes modifications CMDB relationships need to be changed for CIs in the list Completed/Cancelled CMDB relationships modifications	The data in this section is used by the UCMDB integration whenever there are past changes to the values registered for the CI.
Affected Services section > Affected Services	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.
Approvals section> Current Approvals	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. The data displayed includes the following information: • Approval Type • Approval Status • # Approved • # Denied • # Pending
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:

Change Management field descriptions, continued

Label	Description
	• 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.
Cost section > Total Cost	This field indicates the system-calculated total cost of the Change, which is accumulated by the parts and labor cost of the Change itself and its related Change tasks.
Cost section > Currency	Specifies a currency code used by the system to calculate the total cost.
Cost section > Parts table	Specifies the parts used by the Change with their part numbers from the product catalog and the quantity used.
Cost section > Labor table	Specifies the technician who worked on the Change and the actual working hours.
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: • Task No • Phase • Status • Description • Category
Remediation Method	Indicates the remediation method: Full, or Partial.
Remediation Comments	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

Change Management field descriptions, continued

Label	Description
	backing out a change. It is also required in the "Release back out" phase and for the Release Management category in order to close the "Release plan and design" phase.

Chapter 13: Knowledge Management Overview

The HP Knowledge Management application, referred to as Knowledge Management throughout this chapter, supports the Knowledge Management process.

Knowledge Management provides the framework to help you manage information throughout your IT Service Management life cycle. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.

Knowledge Management processes can interact with other Service Manager processes (in particular, Interaction Management, Incident management, and Problem management). The scope of this document is limited to the Knowledge Library and its contents

Topics in this section include:

- "Knowledge Management Within The ITIL Framework" below
- "Knowledge Management Application" on the next page
- "Knowledge Management Process Overview" on page 208
- "Key Interfaces with Other Processes" on page 210
- "Key performance indicators for Knowledge Management" on page 211
- "RACI Matrix For Knowledge Management" on page 212

Knowledge Management Within The ITIL Framework

Knowledge Management (KM) was added to ITIL v3 as part of Service Transition – the ITIL process that addresses the development and deployment of new or changed services. Prior to ITIL v3, the Incident and Problem Management processes were responsible for addressing the management of knowledge. But with the development of a specific Knowledge Management process, ITIL v3 now provides a detailed set of guidelines and workflows for the management of all knowledge in the Service Management life cycle. ITIL v3 also calls for integration of the Knowledge Management process with Service Desk (Interaction Management), Incident Management, and Problem Management.

The goal of Knowledge Management is to enable your organization to efficiently access, update, and share all knowledge that pertains to the Service Management life cycle. Benefits of Knowledge Management include, but are not limited to, the following:

- more efficient handling of knowledge
- the reduced likelihood that multiple stakeholders will attempt to solve the same problem in isolation without first sharing knowledge
- the ability to control the access of sensitive information to certain people

Central to Knowledge Management is a repository known as the Service Knowledge Management System (SKMS). A typical SKMS stores all knowledge in a Knowledge Base. The items in the Knowledge Base are referred to as Knowledge Documents, which can also include a variety of attachment types such as text files and graphics files. It also provides tools for handing important tasks such as generating reports.

HP Service Manager not only acts as the SKMS, it goes one step further by providing Knowledge Center Support (KCS) methodologies out of box. KCS methodologies specify ways to capture information from incidents to be used by analysts in problem solving. It also specifies that knowledge must by definition evolve over time as additional stakeholders review and modify knowledge content.

This *Processes and Best Practices Guide* describes Knowledge Management as the process responsible for providing knowledge to all other IT Service Management processes. Because the number of processes involved is very large, the scope of this document is restricted to those processes related to storing new KM documents and updating, archiving, and retiring existing KM documents.

Knowledge Management Application

The Service Manager Knowledge Management application helps you manage all knowledge related to Interactions, Incidents, and Problems.

Types of Knowledge Documents in Service Manager

Document types are templates for documents in Knowledge Management. Knowledge Management includes several default document types:

- Question/Answer
- Problem-Solution
- Reference

- Error Message/Cause
- External

Knowledge Management Categories

All documents in the knowledge documents knowledge base are assigned to a document category. Categories for knowledge documents are ordered into hierarchies. The document categories order documents into top-level categories and subcategories. Each subcategory has a parent category that is the category immediately above it in the ordered list of categories. A top-level category is also a parent category of the subcategory immediately below it in the ordered list of categories.

Knowledge Groups

Knowledge groups enable you to collect users into groups that have access to work with the same set of documents. A knowledge group might be the user for a department, or a group of document authors, or a special group of users within your organization such as subject matter experts.

You associate a knowledge group with at least one document category or subcategory to give the members of a knowledge group access to documents in the category or subcategory and all subcategories below it. Access privileges can range from search and view to publishing privileges depending upon what knowledge profile(s) you assign to the category.

Knowledge Management Profiles

The Knowledge Management profiles control access to knowledge documents as well as rights for creating, editing, and administering documents.

Within each security profile, there is a direct association between a defined (named) profile and the categories and sub-categories for which the selected capabilities apply. Each security profile maps to a document category or sub-category. A user with that profile has access to the documents specified by the profile-to-category mapping and all subcategories in that branch of the category tree.

Profiles can be modified to select only some of the available capabilities for a profile, effectively creating sub-profiles. For example, some users may not be allowed to publish knowledge documents externally as well as internally.

The out-of-box KM security profiles are briefly described in the following table:

Contribute And Approve Knowledge/Change Request Process

KM Profile	Privileges
DEFAULT	With this profile, a user can search and view externally published knowledge documents for those documents in categories to which this profile has access. They can also submit feedback on these documents.
INTERNAL USER	With this profile, a user can search and view externally published knowledge documents for those documents in categories to which this profile has access. They can also search and view internally approved knowledge documents for those documents in categories to which this profile has access. They can also submit feedback on these documents.
KCS I	Author and contribute knowledge documents.
KCS EDITOR	Editor Author knowledge documents and edit working copy documents in the workflow for those categories to which this profile has access.
KCS II	Author knowledge documents, contribute knowledge documents, edit published documents without placing them in workflow (edit in place), and publish documents internally only. Also, view adaptive learning data when adaptive learning is enabled in the system.
KCS III	Author knowledge documents, contribute knowledge documents, edit published documents without placing them in workflow (edit in place), and publish documents internally and externally. Also, view adaptive learning data when adaptive learning is enabled in the system.
KM ADMIN	Author knowledge documents, contribute knowledge documents, edit published documents without placing them in workflow (edit in place), and publish documents internally and externally. Also, view adaptive learning data when adaptive learning is enabled in the system.

Generic OOB Knowledge Management Document Phases

KM documents pass through the following generic out-of-box phases:

1. **Draft**
   A Knowledge Contributor creates a draft document by first selecting one of the following document types:

   - **Error Message/Cause**: a specific error message a user encountered and what the user was doing when the error occurred

   - **External**: files, such as text or graphic files, that can be associated with incidents and problems

- **Question/Answer**: a general question and its corresponding answer
- **Problem/Solution**: a specific problem, including its probable cause, and a corresponding solution
- **Reference**: general information
  Once a draft is created, the Knowledge Document is said to be a **Working copy**. Note that in the Service Manager Knowledge Management application, a working copy of a published document has an "R" appended to the document ID. A new document submitted to be published is also considered a working copy while it is in workflow waiting to be published, but there is no "R" appended to the document ID.

2. **Triage**
   After the contributor enters the relevant details and submits the draft document, it enters the Triage state. The purpose of the Triage state is to allow a KM analyst to review the submission and determine if it would make an appropriate document. The analyst can also perform minor modifications of the content to ensure stylistic quality. If the document is acceptable, the analyst submits it to a specific KM expert for revision.

3. **Revise**
   The purpose of the Revise state is to give a subject matter expert the chance to add or modify content that would improve the document. After revising the document, the KM expert submits the document for review to the KM team.

4. **Review**
   The purpose of the Review state is to give the KM team a chance to finally decide if the document is ready for publication. The KM team can send the document back for further revision or to accept the document.

5. **Conclude**

   > **Note:** This is the Publish phase in the out-of-box KM workflow.

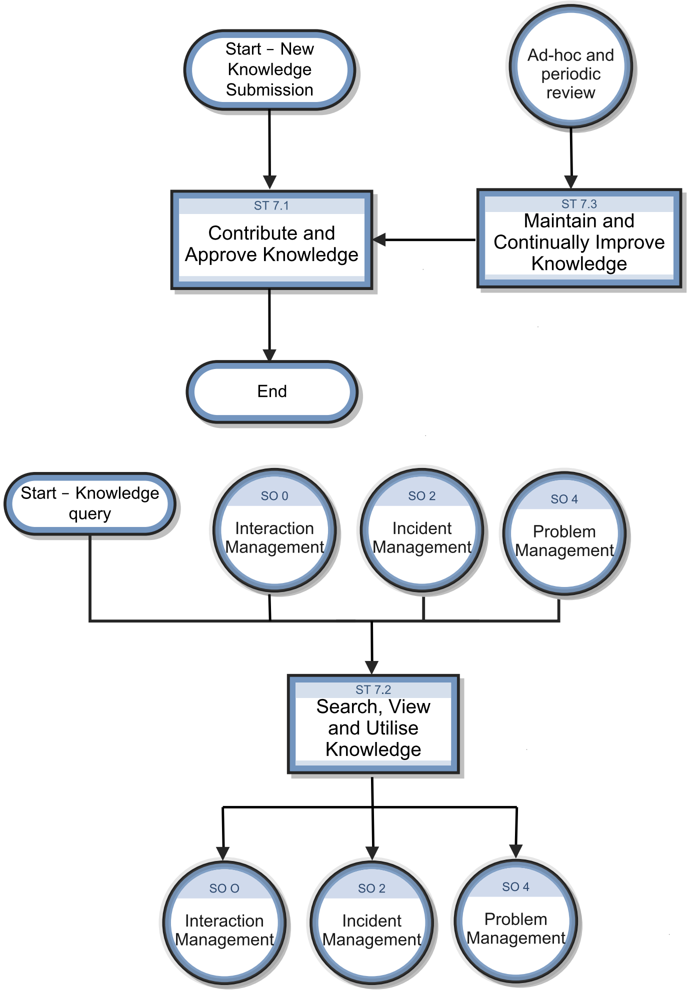
   The purpose of the Conclude stage is to allow the assigned owner on the KM team to determine what to do with the document. The owner has the following options:

   - If the document is new, the owner can approve and publish the submission, or terminate the KM record to prevent publication of the document.
   - If the document already exists and was resubmitted for revision and review, the owner can publish the revised version, revert to the original version, or retire the document.

Documents can also be retired when they are no longer useful. A retired document is a knowledge document that is no longer searched during a knowledge base search.

Knowledge Management Process Overview

A general overview of the Knowledge Management processes and workflows is depicted in the following figure. Workflows are described in detail in "Knowledge Management Workflows".



Knowledge Management User Roles

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

Knowledge Management User Roles

Role	Responsibilities
Knowledge Management Process Owner	• Accountable for the definition, management, governance and improvement of the KM Process • Ensures that the KM process and working practices are effective and efficient • Ensures that all stakeholders are sufficiently involved in the KM process • Ensures that (business) management is sufficiently informed as to the volume, impact and cost of Knowledge • Ensures tight linkage between the KM process and other related processes
Knowledge Manager	• Implementation and ongoing management of the Knowledge Management process • Championing the Knowledge Management process with people at all levels • Management of Knowledge Analysts • Ensuring process efficiency and consistency • Final QA and approval of all Knowledge Submissions • Deciding the scope of publishing (external and / or internal) • Continual improvement of the Knowledge Library and process • Fast tracking urgent 'Hot News' notices through the KM process • Reviewing KM reports • Identifying, allocating and tracking continual improvement actions and maintenance activities
Knowledge Expert	• Reviewing and amending Knowledge Submissions • Rejecting Knowledge Submissions based on technical content • Assisting with reviews of Knowledge Documents for currency and relevance
Knowledge Analyst	• Administering the KM process • Reviewing Knowledge Candidates for basic content, spelling, format, readability, duplication and editing to achieve a consistent quality level • Rejecting inappropriate or duplicated Knowledge Submissions

Knowledge Management User Roles, continued

Role	Responsibilities
	• Co-ordinating Knowledge Expert reviews and reviewing Knowledge Document feedback and identifying improvements • Producing and distributing KM reports • Driving periodic reviews of Knowledge and co-ordinating and / or performing improvement actions • Retiring Knowledge Documents no longer deemed relevant
Knowledge Contributor	• Identifying Knowledge Submissions • Identifying changes required to existing Knowledge Documents • Submitting new or revised Knowledge Submissions • Assisting with reviews of Knowledge Documents for currency and relevance
Knowledge User	• Maintaining awareness of the KM facilities • Searching the Knowledge Base for solutions • Providing feedback on Knowledge Documents **Note:** • Self-Service will only access the Knowledge Library • Operator record search will access Interaction, Incident, Known Error and Knowledge libraries

Key Interfaces with Other Processes

The following table shows how Knowledge Management is linked with other Service Manager processes.

Input and output for Knowledge Management

Process	Description
SO 0 – Interaction Management	Knowledge documents may be used in the resolution of Incidents, either via the Service Desk or self-service. Feedback on the knowledge documents will feed in to the Knowledge Management process.
SO 2 – Incident Management	During the Incident resolution process, KM documents can be submitted that specify how an analyst found a resolution or workaround.

Input and output for Knowledge Management, continued

Process	Description
SO 4 – Problem Management	Information on Known Errors and workarounds may be used to create Knowledge Documents.

Key performance indicators for Knowledge Management

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

Key Performance Indicators for Knowledge Management

Title	Description
Number of KM documents created	The total number of KM documents in your organization will grow over time; however, older KM documents will gradually become outdated and should be retired. Monitor the number of newly created documents to determine the optimal rate of growth over a period of time.
Number of times a KM document is accessed	A useful document is accessed frequently. Use this indicator to figure out which documents are the most and least useful.
Number of KM documents used to resolve Interactions	KM documents should ultimately lead to resolutions. Monitor the number of KM documents that lead to resolutions of Interactions to help determine how successfully your Service Desk is able to access and reuse knowledge.
Number of KM documents used to resolve Incidents	Monitor the number of KM documents that lead to resolutions of Incidents to help determine how successfully KM documents help resolve serious issues that have been escalated to Incidents.
Number of KM documents with an expired review date	To ensure the efficiency of the document publication process, monitor the number of documents that have not been reviewed in a timely manner.

RACI Matrix For Knowledge 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 Knowledge Management is shown in the following table.

RACI Matrix For Knowledge Management

Process ID	Activity	Knowledge Contributor	Knowledge Analyst	Knowledge Expert	Knowledge Manager	Knowledge User
ST 7.1	Contribute and Approve Knowledge	R	R	C	A/R	
ST 7.2	Search, View and Utilise Knowledge				A	R
ST 7.3	Maintain and Continually Improve Knowledge	R	R	R	A/R	

Chapter 14: Knowledge Management Workflows

The Knowledge Management process collects, organizes, structures and distributes knowledge for ongoing use. It is responsible for ensuring that an organization can archive and retrieve knowledge in an efficient manner.

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

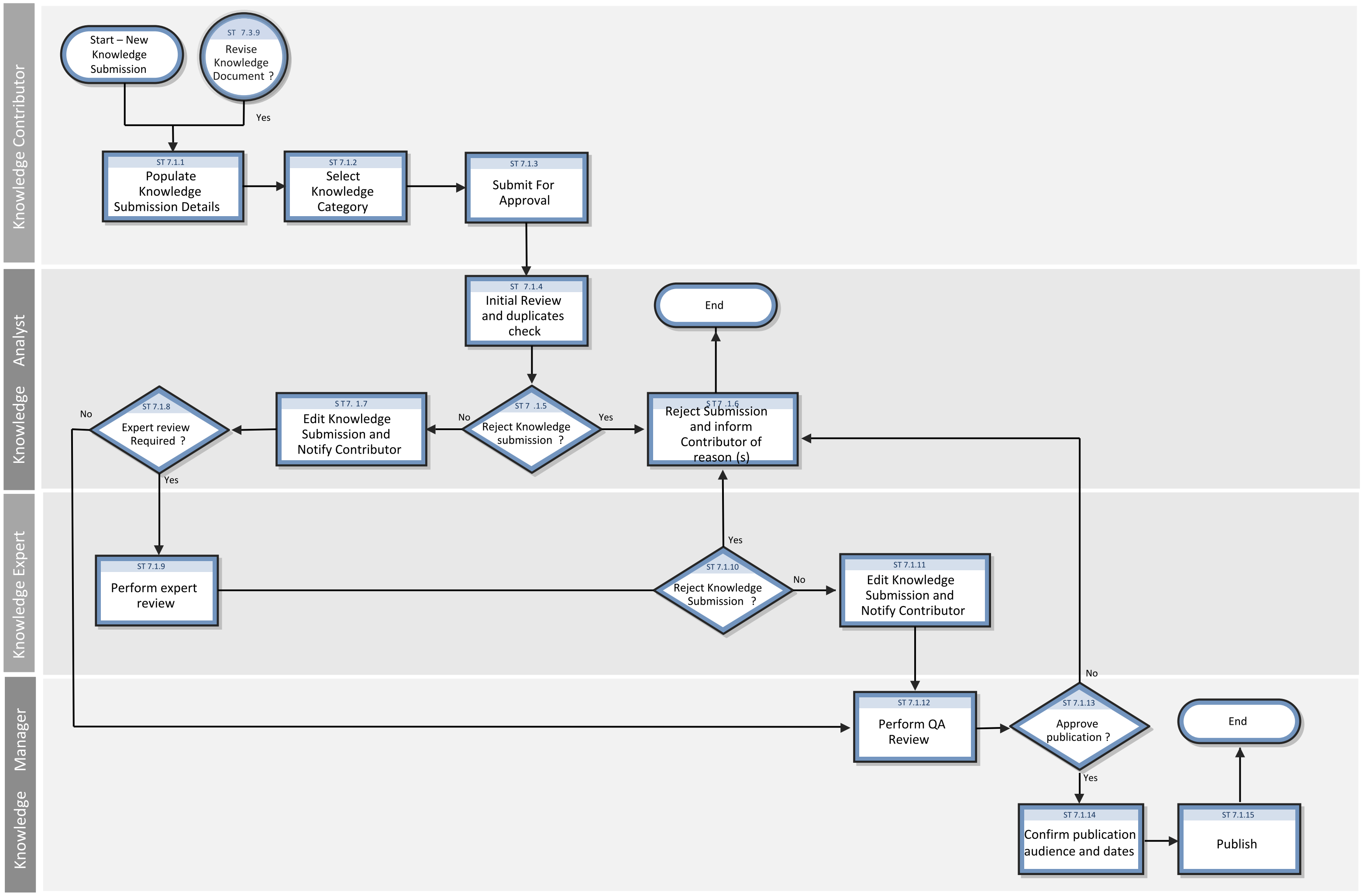
- "Contribute and Approve Knowledge Document (process ST 7.1)" on the next page
- "Search, View and Utilize Knowledge Document (Process ST 7.2)" on page 218
- "Maintain and Continually Improve Knowledge (Process ST 7.3)" on page 221

Contribute and Approve Knowledge Document (process ST 7.1)

The Contribute and Approve Knowledge Document process starts with the submission of a KM document. You can contribute a knowledge document by authoring knowledge articles or using external documents that are uploaded into a knowledge base. You can use the rich-text editor to author documents, and you can add documents as attachments that can include images, text files, Word files, or PDFs.

- The process begins when a contributor creates a new submission or revising an existing knowledge document. The contributor selects a documentation type, enters basic details, selects a category type, and submits the draft for review by a Knowledge Analyst.
- The analyst can edit, accept, or reject the document. If necessary, the document can be passed to a Knowledge Expert, who can also edit, accept, or reject it. The Knowledge Expert is typically a subject-matter expert with more in depth understand of a give topic and the ability to determine the accuracy and currency of the KM document.
- The Knowledge Manager makes the final decision about whether to accept the document or return it for further revision. If the document meets all KM publication criteria, the Knowledge Manager accepts and publishes the document.

The Contribute And Approve KM Doc/Change Request Workflow is illustrated in the following figure:


Knowledge Contributor
Start – New Knowledge Submission
ST 7.3.9
Revise Knowledge Document ?
Yes
ST 7.1.1
Populate Knowledge Submission Details
ST 7.1.2
Select Knowledge Category
ST 7.1.3
Submit For Approval
Knowledge Analyst
ST 7.1.4
Initial Review and duplicates check
End
No
ST 7.1.8
Expert review Required ?
ST7. 1.7
Edit Knowledge Submission and Notify Contributor
No
ST 7 .1.5
Reject Knowledge submission ?
Yes
ST7 .1.6
Reject Submission and inform Contributor of reason (s)
Yes
Knowledge Expert
ST 7.1.9
Perform expert review
Yes
ST 7.1.10
Reject Knowledge Submission ?
No
ST 7.1.11
Edit Knowledge Submission and Notify Contributor
Knowledge Manager
No
ST 7.1.12
Perform QA Review
ST 7.1.13
Approve publication ?
End
Yes
ST 7.1.14
Confirm publication audience and dates
ST 7.1.15
Publish

Contribute And Approve Knowledge/Change Request Process

Process ID	Procedure or Decision	Description	Role
ST 7.1.1	Populate Knowledge details	Enter details of the Knowledge Submission into Service Manager. Suggestions for new or improved KM documents can be received from a number of areas including Incident and Problem Management. Go to ST 7.1.2 to select the appropriate Knowledge category.	Knowledge Contributor
ST 7.1.2	Select Knowledge category	Select the appropriate category from those available within Service Manager. Go to ST 7.1.3 to submit the Knowledge Submission.	Knowledge Contributor
ST 7.1.3	Submit for approval	Submit the Knowledge Submission for approval by the Knowledge team. Go to ST 7.1.4 in order for the Knowledge Analyst to perform an initial review and check for duplicates.	Knowledge Contributor
ST 7.1.4	Initial review and duplicates check	The Knowledge Submission is reviewed to ensure all required information has been provided and in the correct format. A check is also done against other recent Knowledge Submissions to avoid duplication of effort. Go to ST 7.1.5 to determine whether to reject the Knowledge Submission.	Knowledge Analyst
ST 7.1.5	Reject Knowledge Submission?	The Knowledge Submission will be rejected if the Knowledge Analyst feels it is not valid or if it is a duplication of another existing proposal. If yes, go to ST 7.1.6 to inform the Knowledge Contributor of the reasons for rejection. If no, go to ST 7.1.7 to edit the Knowledge Submission.	Knowledge Analyst
ST 7.1.6	Retire Knowledge Submission and inform Contributor of reason(s)	Inform the Knowledge Contributor of the reasons for the Knowledge Submission being rejected. The ‘Contribute and Approve Knowledge’ process ends.	Knowledge Analyst
ST 7.1.7	Edit Knowledge Submission and notify Contributor	Add any comments / additional information to the Knowledge Submission ready for further review and approval, and notify the Knowledge Contributor. Go to ST 7.1.8 to determine whether an expert review is required.	Knowledge Analyst
ST 7.1.8	Expert Review Required?	Some Knowledge Submissions can be managed by the Knowledge team only. If the Knowledge Submission refers to a specialised area, an expert will be asked to review and approve it. If yes, go to ST 7.1.9 for the Knowledge Expert to review the Knowledge Submission. If no, go to ST 7.1.12 for	Knowledge Analyst

Contribute And Approve Knowledge/Change Request Process, continued

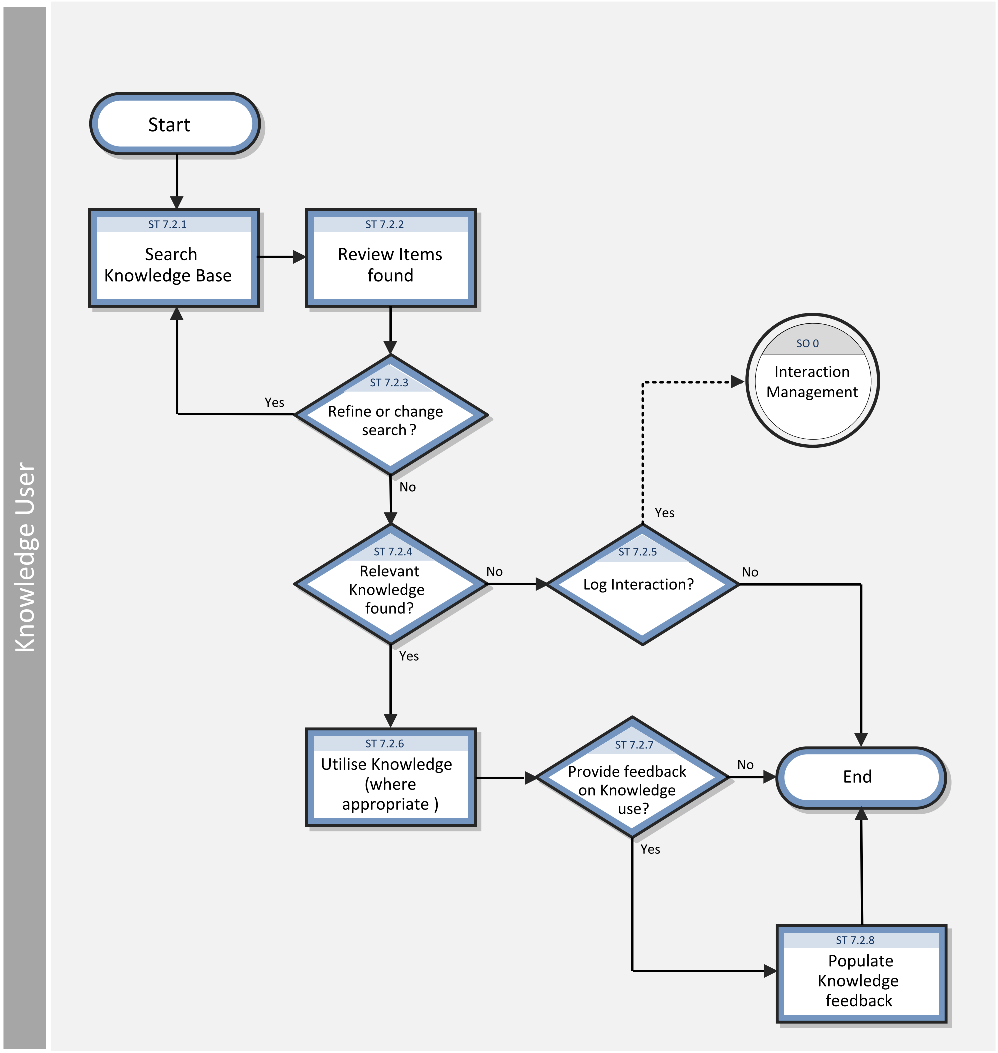
Process ID	Procedure or Decision	Description	Role
		the Knowledge Manager to perform a QA review.	
ST 7.1.9	Perform Expert review	Review the Knowledge Submission. Go to ST 7.1.10 to determine whether to reject the Knowledge Submission.	Knowledge Expert
ST 7.1.10	Reject Knowledge Submission?	If the Knowledge Expert believes the Knowledge Submission is not valid, they can decide to reject it and provide reasons which will be provided to the Knowledge Contributor. If yes, go to ST 7.1.6 to inform the Knowledge Contributor of the rejection reason. If no, go to ST 7.1.11 to edit the Knowledge Submission.	Knowledge Expert
ST 7.1.11	Edit Knowledge Submission and notify Contributor	Add comments / additional information to the Knowledge Submission ready for further review and approval. Notify the Knowledge Contributor if any amendments have been made. Go to ST 7.1.12 in order for the Knowledge Manager to perform a QA review.	Knowledge Expert
ST 7.1.12	Perform QA Review	The Knowledge Manager performs a final review of the Knowledge Submission to ensure that it is consistent with the quality and format of the rest of the Knowledge Documents. Go to ST 7.1.13 to decide whether or not to approve the Knowledge Submission for publication.	Knowledge Manager
ST 7.1.13	Approve Publication?	Once the Knowledge Manager is sure that the Knowledge Submission has had the necessary checks and approvals, they will decide whether or not to publish it. If yes, go to ST 7.1.14 to confirm the correct audience & dates for publication. If no, go to ST 7.1.6 for the Knowledge Analyst to inform the Knowledge Contributor of the rejection reason.	Knowledge Manager
ST 7.1.14	Confirm publication audience and dates	Confirm the appropriate audience for the Knowledge Submission and if there are any restrictions or deadlines associated with its publication. Go to ST 7.1.15 to publish.	Knowledge Manager
ST 7.1.15	Publish	Publish the Knowledge Submission to the Knowledge Base. The ‘Contribute and Approve Knowledge’ process ends.	Knowledge Manager

Search, View and Utilize Knowledge Document (Process ST 7.2)

The Knowledge Base is the central repository of the Knowledge Management system. Service Manager provides powerful search and retrieval functionality for accessing, retrieving, and displaying knowledge documents. Searches can be performed using Filters and even Boolean searches are allowed.

Each type of Knowledge Bases has different fields that are indexed for searching, so specific search parameters that match the fields in the knowledge base must be provided. For example, the knowledge articles have a title and author field. When you view an incident, the out-of-box system displays the incident number, incident description, and solution for closed incidents.

Search, View and Utilize Knowledge process is illustrated in the following figure:



Search, View And Utilize Knowledge Process

Process ID	Procedure or Decision	Description	Role
ST 7.2.1	Search Knowledge Base	Enter search criteria into the tool. Search queries can be entered by users through the Self Service functionality or by Operators from the Interaction, Incident and Problem Management modules (this is shown in grey on the process flow as they are not always present when this process is followed.). Go to ST 7.2.2 to review items found.	Knowledge User
ST 7.2.2	Review Items Found	Review search results and determine whether any are appropriate. Go to ST 7.2.3 to refine or amend the search, if necessary.	Knowledge User
ST 7.2.3	Refine or change search	If appropriate Knowledge Documents have not been returned, the search criteria can be amended to obtain better results. If yes, go to ST 7.2.1 to search the Knowledge Base again. If no, go to ST 7.2.4 to determine whether relevant Knowledge has been found.	Knowledge User
ST 7.2.4	Relevant Knowledge Found?	Has a Knowledge Document been returned that is helpful and relevant to the query? If yes, go to ST 7.2.6 to Utilize Knowledge where appropriate. If no, go to ST 7.2.5 to determine whether to log an Interaction.	Knowledge User
ST 7.2.5	Log Interaction?	If a suitable Knowledge Document was not found, an Interaction may need to be raised to deal with the issue that was being researched. If yes, go to Interaction Management (SO 0.1.1). If no, the ‘Search, View and Utilize Knowledge’ process ends.	Knowledge User
ST 7.2.6	Utilize Knowledge (where appropriate)	Apply the Knowledge where appropriate. Go to ST 7.2.7 to determine whether to provide feedback on the Knowledge Document.	Knowledge User
ST 7.2.7	Provide feedback on Knowledge Use?	Feedback is monitored for key aspects such as quality and availability of the Knowledge Documents. If yes, go to ST 7.2.8 to populate Knowledge feedback. If no, the ‘Search, View and Utilize Knowledge’ process ends.	Knowledge User
ST 7.2.8	Populate Knowledge feedback	Populate feedback on the Knowledge Document used. The ‘Search, View and Utilize Knowledge’ process ends.	Knowledge User

Maintain and Continually Improve Knowledge (Process ST 7.3)

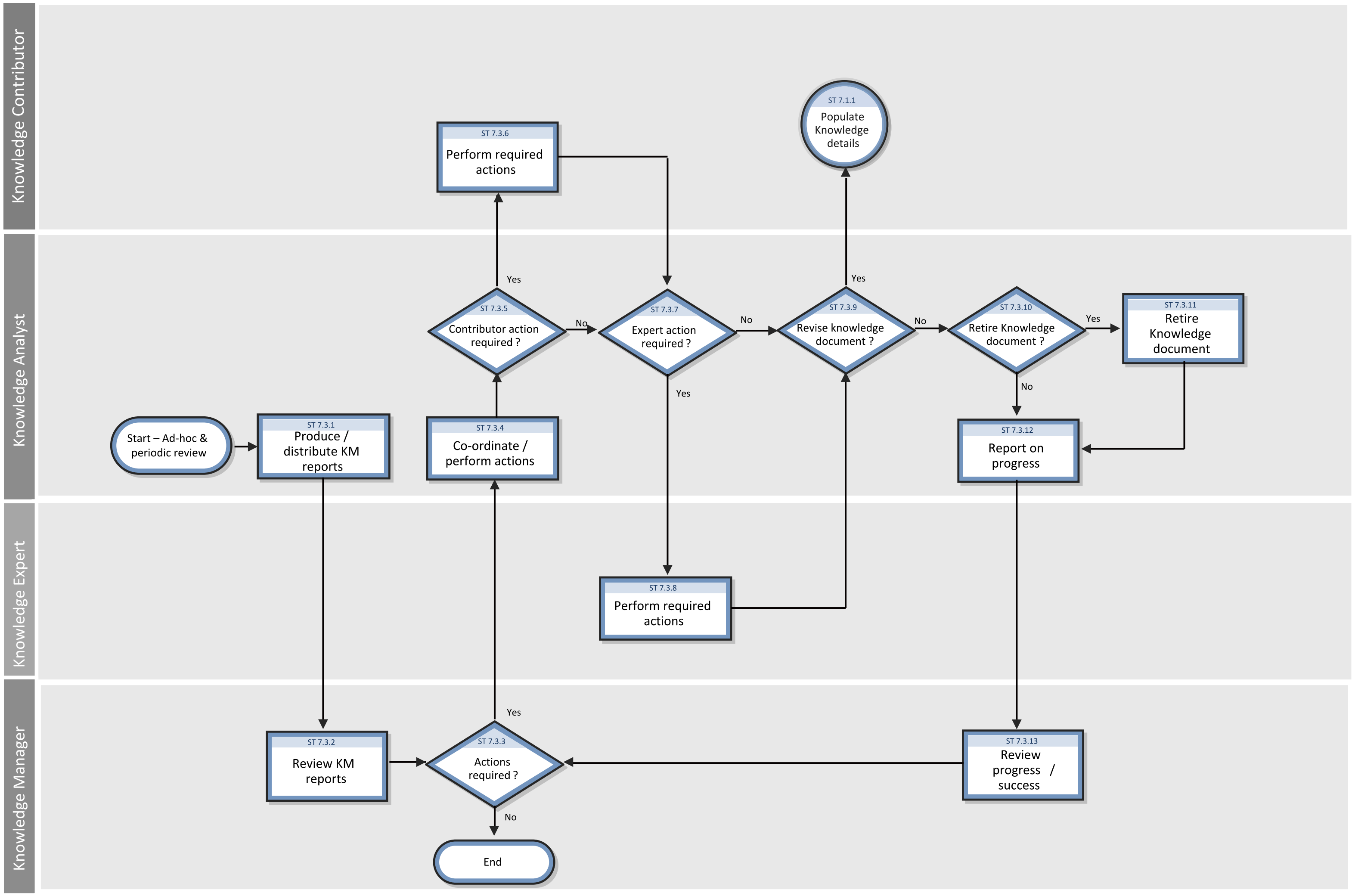
The Maintain And Continually Improve Knowledge process:

- Records the details of new knowledge (documents)
- Updates existing knowledge (documents) where there is any inaccuracy or incompleteness
- Removes obsolete knowledge (documents)

The process is performed by the Knowledge Contributor, Knowledge Analyst, Knowledge Expert, or Knowledge Manager.

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

The Maintain and Continually Improve Knowledge Workflow is illustrated in the following figure:


Knowledge Contributor
Knowledge Analyst
Knowledge Expert
Knowledge Manager
Start – Ad-hoc & periodic review
ST 7.3.1 Produce / distribute KM reports
ST 7.3.2 Review KM reports
ST 7.3.3 Actions required ?
Yes
No
End
ST 7.3.4 Co-ordinate / perform actions
ST 7.3.5 Contributor action required ?
Yes
No
ST 7.3.6 Perform required actions
ST 7.3.7 Expert action required ?
Yes
No
ST 7.3.8 Perform required actions
ST 7.3.9 Revise knowledge document ?
Yes
No
ST 7.1.1 Populate Knowledge details
ST 7.3.10 Retire Knowledge document ?
Yes
No
ST 7.3.11 Retire Knowledge document
ST 7.3.12 Report on progress
ST 7.3.13 Review progress / success

Maintain and Continually Approve Knowledge

Process ID	Procedure or Decision	Description	Role
ST 7.3.1	Produce / distribute KM reports	Produce and distribute KM reports to the Knowledge Manager. Go to ST 7.3.2 for the Knowledge Manager to review the KM reports.	Knowledge Analyst
ST 7.3.2	Review KM reports	Review the reports for any issues with the tool or process. Go to ST 7.3.3 to determine required actions.	Knowledge Manager
ST 7.3.3	Actions required?	Identify whether any additional actions need to be taken. If yes, go to ST 7.3.4 to co-ordinate / perform actions. If no, the ‘Maintain and Continually Improve Knowledge’ process ends.	Knowledge Manager
ST 7.3.4	Co-ordinate / perform actions	Review the identified actions and resolve any that do not need Knowledge Contributor or Knowledge Expert involvement. Go to ST 7.3.5 to determine whether action is required by the Knowledge Contributor.	Knowledge Analyst
ST 7.3.5	Contributor action required?	If yes, go to ST 7.3.6 for the Knowledge Contributor to perform the required actions. If no, go to ST 7.3.7 to determine whether action is required by a Knowledge Expert.	Knowledge Analyst
ST 7.3.6	Perform required actions	Implement appropriate actions to resolve the issue identified in the KM report. Go to ST 7.3.7 to determine whether action is required by a Knowledge Expert.	Knowledge Contributor
ST 7.3.7	Expert action required?	If yes, go to ST 7.3.8 for the Knowledge Expert to perform the required actions. If no, go to ST 7.3.9 to determine whether to revise the Knowledge Document.	Knowledge Analyst
ST 7.3.8	Perform required actions	Implement appropriate actions to resolve the issue identified in the KM report. Go to ST 7.3.9 to determine whether to revise the Knowledge Document.	Knowledge Expert
ST 7.3.9	Revise Knowledge Document?	If yes, go to ST 7.1.1 for the Knowledge Contributor to populate Knowledge details. Note: The Knowledge Analyst is the Knowledge Contributors role in this scenario. If no, go to ST 7.3.10 to determine whether to retire the Knowledge Document.	Knowledge Analyst
ST 7.3.10	Archive Knowledge Document?	If yes, go to ST 7.3.11 to retire the Knowledge Document. If no, go to ST 7.3.12 to report on progress against actions.	Knowledge Analyst

Maintain and Continually Approve Knowledge, continued

Process ID	Procedure or Decision	Description	Role
ST 7.3.11	Retire Knowledge Document	Archive the Knowledge Document in order for it to be no longer available in searches of the Knowledge Base. Go to ST 7.3.12 to report on progress.	Knowledge Analyst
ST 7.3.12	Report on progress	Provide the Knowledge Manager with a progress report on any outstanding actions. Go to ST 7.3.13 in order for the Knowledge Manager to review progress/success.	Knowledge Analyst
ST 7.3.13	Review progress/success	Review progress on actions identified and determine whether any additional actions are required. Go to ST 7.3.3 determine whether additional actions are required.	Knowledge Manager

Chapter 15: Knowledge Management Details

HPService Manager uses the Knowledge Management application to enable the Knowledge Management process. The main function of Knowledge Management is to record, store, update and change Knowledge Documents for use throughout the organization.

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

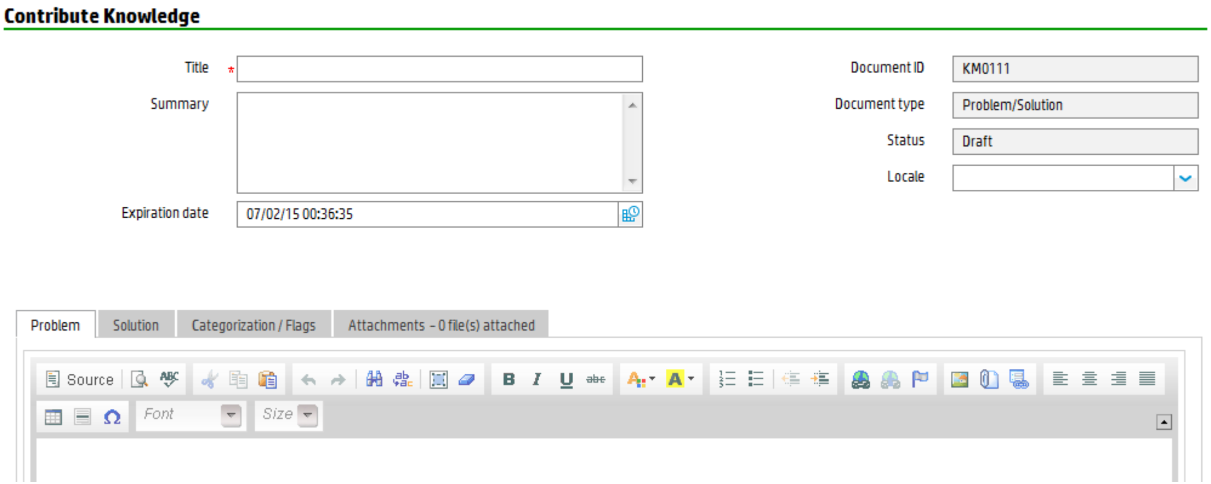
Topics in this section include:

- "Knowledge Management Form - Contribute Knowledge" below
- "Knowledge Management Form - Search Knowledgebase (Advanced Search)" on the next page

Knowledge Management Form - Contribute Knowledge

The following figure shows the Service Manager KM Contribute Knowledge form for the Problem/Solution document type. The form is used to contribute knowledge (a new KM Document request). As with any new KM document, you must complete the required fields before you can save the record. See the following table for a list and description of the fields on this form.

The Contribute Knowledge form is illustrated in the following screenshot:



Contribute Knowledge

Title *		Document ID	KM0111
Summary		Document type	Problem/Solution
		Status	Draft
		Locale	
Expiration date	07/02/15 00:36:35		

The following table describes the Contribute Knowledge form for the Problem/Solution document type.

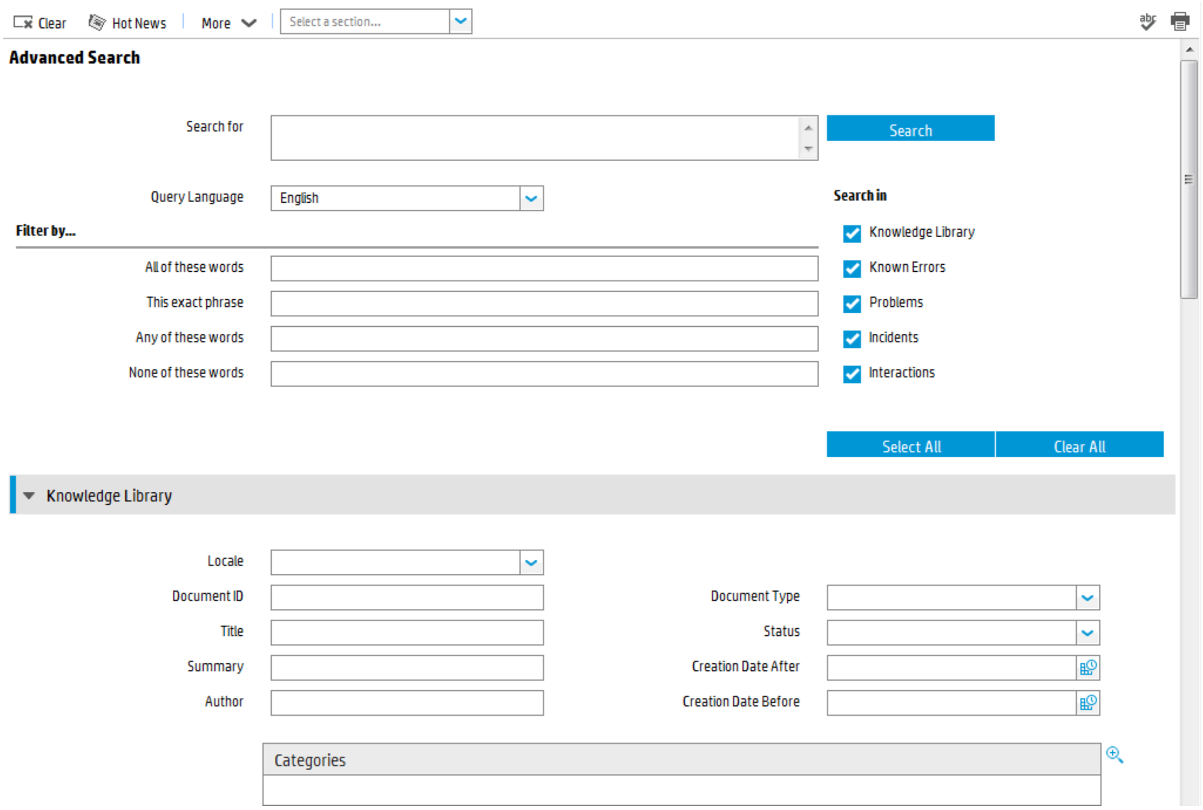
Contribute Knowledge form field descriptions

Label	Description
Title	The title of the document. The title should accurately describe the content of the document.
Summary	A summary of the document.
Expiration date	The date that the KM document will automatically expire.
Document ID	Service Manager creates the ID of the document automatically.
Document type	There are five Document Types: Error Message/Cause; External; Question/Answer; Problem/Solution; and Reference.
Status	The KM document’s current state in the KM workflow.
Locale	The language used by the search engine when searching and indexing. The default locale is English.

Knowledge Management Form - Search Knowledgebase (Advanced Search)

The following figure shows the Search Knowledgebase (Advanced Search) form. This form enables users to search for knowledge documents from these knowledgebases: Knowledge Library, Known Errors, Problems, Incidents, and Interactions. To access this form, navigate to **Knowledge Management** > **Search Knowledgebase**, and then click the **Advanced...** button.

The Search Knowledgebase (Advanced Search) form is illustrated in the following screenshot:



Query Language: English

All of these words
This exact phrase
Any of these words
None of these words

☑ Knowledge Library
☑ Known Errors
☑ Problems
☑ Incidents
☑ Interactions

The following table describes the fields on this form.

Contribute Knowledge form field descriptions

Label	Description
Clear	This button clears existing search criteria. If you return to the simple search form without clicking this button, existing search criteria will remain.
Search for	The text string to search for.
Query Language	Indicates the dictionary that the Search Engine will use for Natural Language breakdown, thesaurus, and stemming. The default language is English. Normally this should be the language of the text string in the **Search for** text box. **Note:** Only languages with the Active for Knowledge Management option enabled in their Language Identification record are available from the Query Language list.
Filter by	Use this section to narrow down your search. Note that all “Filter by” words/phrases are not highlighted in search results. **All of these words**: Search for documents that contain every one of these words. **This exact phrase**: Search for documents that contain this phrase exactly. These

Contribute Knowledge form field descriptions , continued

Label	Description
	words are not expanded with a thesaurus. **Any of these words**: Search for documents that contain any one of these words. **None of these words**: Search for documents that do not contain any of these words.
Search in	This section specifies the knowledgebases to search: Knowledge Library, Known Errors, Problems, Incidents, and Interactions.
Knowledge Library	This section contains fields from the Contribute Knowledge form that you can use as a filter when searching for knowledge documents stored in the kmdocument table. **Note:** • Only languages with the **Active for Knowledge Management** option enabled in their Language Identification record are available from the Locale list. Use the Locale field in combination with the Query Language field. For example, if you want to search for a Japanese document (whose Locale is Japanese) that contains a French word, specify Query Language as French, and Locale as Japanese. • Use the **Add** and **Remove** buttons to add and remove Categories as needed. • Administrators can also use the **HP Service Manager Table Query** field in the Knowledge_Library knowledgebase to limit end user’s searches to partial KM documents. Out-of-the-box, the query is: `status ~= "draft" and status ~="retired"`, which means users can only search for KM documents whose status is not Draft or Retired.
Known Errors	This section contains fields from the knownerror table that you can use as a filter when searching for Known Error knowledge records.
Problems	This section contains fields from the rootcause table that you can use as a filter when searching for Problem knowledge records.
Incidents	This section contains fields from the probsummary table that you can use as a filter when searching for Incident knowledge records.
Interactions	This section contains fields from the incidents table that you can use as a filter when searching for Interaction knowledge records.

Chapter 16: Configuration Management Overview

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

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

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

Topics in this section include:

- "Configuration Management within the ITIL framework" below
- "Configuration Management application " on the next page
- "HP Universal Configuration Management Database"
- "Configuration Management process overview" on page 236
- "Input and output for Configuration Management" on page 239
- "Key performance indicators for Configuration Management" on page 240
- "RACI matrix for Configuration Management" on page 242

Configuration Management within the ITIL framework

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

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

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

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

Effective Configuration Management provides the following benefits:

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

Configuration Management application

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

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

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

Configuration Management enables you to do the following:

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

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

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

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

HP Universal Configuration Management Database

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

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

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

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

- By default, the integration automatically updates the managed fields of Service Manager CI records as part of the regular UCMDB synchronization schedule. You can choose the option to configure the integration to automatically create change or incidents instead.

- You can view the current actual state of a CI by looking at the Actual State section in the Service Manager CI record. For more information see "Baselines" below, "Managed state" on page 234 and "Actual state" on page 234.

- You can use the Service Manager View in UCMDB option to log in to the UCMDB system and view the current CI attributes from UCMDB. A Service Manager user must have a valid UCMDB user name and password to log in to the UCMDB system.

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

Baselines

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

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

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

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

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

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

Baseline section

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

Managed state

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

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

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

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

Managed State section

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

Actual state

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

Actual State section

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

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

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

CI relationships

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

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

CI Relationship section (CI visualization)

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

Configuration Management process overview

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

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

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

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

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

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

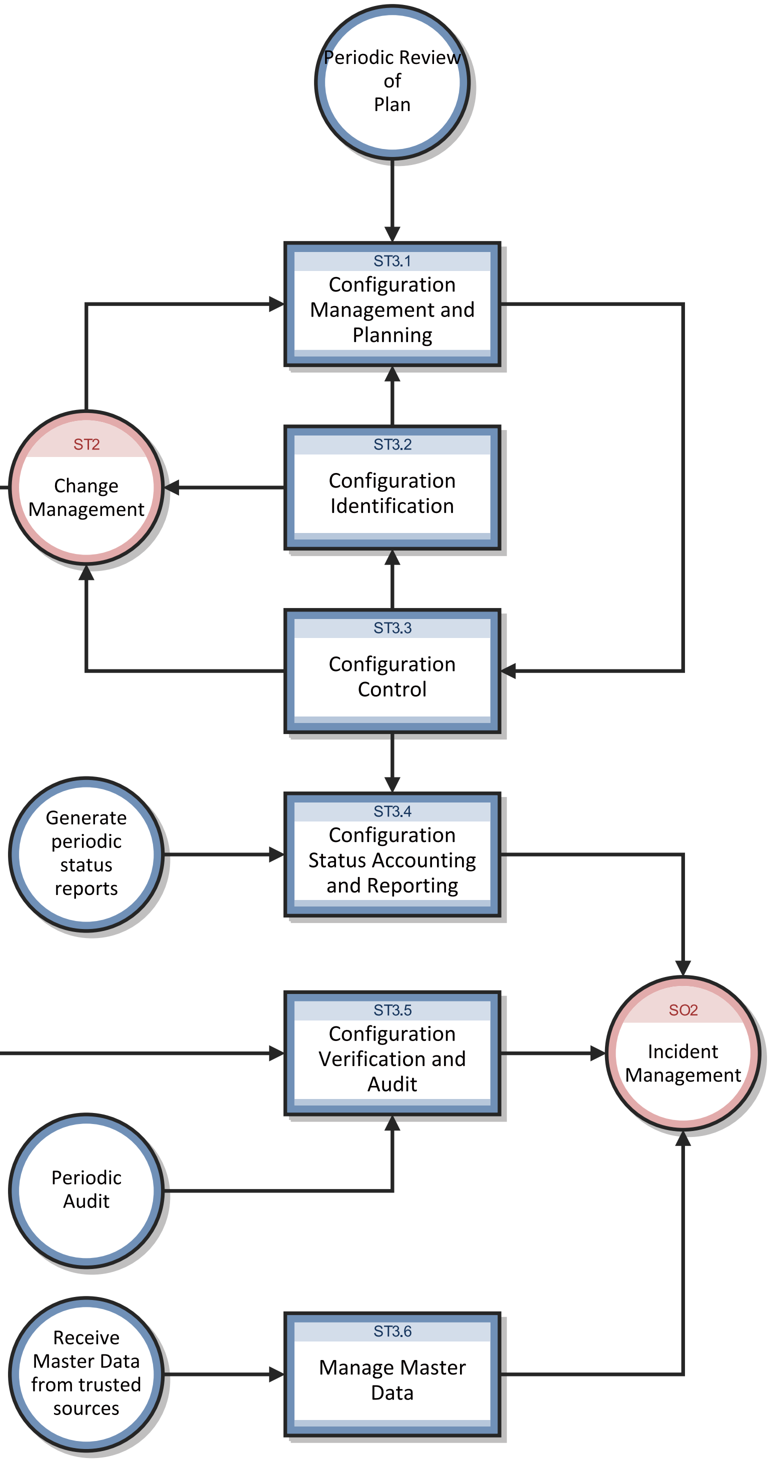
Configuration Management comprises five basic activities. The Configuration Management process encompasses all of these activities and ensures that assets are tracked and monitored effectively. The basic activities within the scope of Configuration Management are:

- "Configuration Management Planning (process ST 3.1)" on page 244 — includes the activities that enable you to plan the function, scope, and objectives of Service Manager for your organization.
- "Configuration Identification (process ST 3.2)" on page 250 — includes the activities that enable you to identify and label all of your company’s existing IT components. The information you track

includes asset identification, contact, asset network relationship, and model or version data. Enter this information into the database.

- *Inventory maintenance*
  - "Configuration Control (process ST 3.3)" on page 255 — includes the activities that enable you to ensure that all information regarding your IT components is kept up to date and accurate. Components can be added, modified, or removed only through controlling documentation, such as an approved Request for Change (RFC).
  - "Master data management (process ST 3.6)" on page 271 — includes the activities that enable you to reconcile master reference data managed in other administrations.
- "Configuration Status Accounting and Reporting (process ST 3.4)" on page 260 — includes the activities that enable you to run reports of the current and historical data that is concerned with each IT component throughout its life cycle. Status accounting makes changes to components that can be tracked.
- "Configuration Verification and Audit (process ST 3.5)" on page 266 — includes the activities that enable you to check and verify physical existence of IT components and ensure that they are correctly recorded in the database.

A general overview of the Configuration Management processes and workflows is depicted in the figure below. They are described in detail in "Configuration Management Workflows".


Periodic Review of Plan
ST3.1
Configuration Management and Planning
ST2
Change Management
ST3.2
Configuration Identification
ST3.3
Configuration Control
Generate periodic status reports
ST3.4
Configuration Status Accounting and Reporting
ST3.5
Configuration Verification and Audit
SO2
Incident Management
Periodic Audit
Receive Master Data from trusted sources
ST3.6
Manage Master Data

Configuration Management user roles

The following figure describes the responsibilities of the Configuration Management user roles.

Configuration Management user roles

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

Input and output for Configuration Management

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

Input and output for Configuration Management

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

Key performance indicators for Configuration Management

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

Key Performance Indicators for Configuration Management

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

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

ITIL V3 key performance indicators

The following are ITIL V3 KPIs for Configuration Management:

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

COBIT 4.1 key performance indicators

The following are the COBIT 4.1 KPIs for Configuration Management:

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

- Percent of configuration items meeting specified service levels for performance, security, and availability

RACI matrix for Configuration Management

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

RACI matrix for Configuration Management

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

Chapter 17: Configuration Management Workflows

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

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

- "Configuration Management Planning (process ST 3.1)" on the next page
- "Configuration Identification (process ST 3.2)" on page 250
- "Configuration Control (process ST 3.3)" on page 255
- "Configuration Status Accounting and Reporting (process ST 3.4)" on page 260
- "Configuration Verification and Audit (process ST 3.5)" on page 266
- "Master data management (process ST 3.6)" on page 271

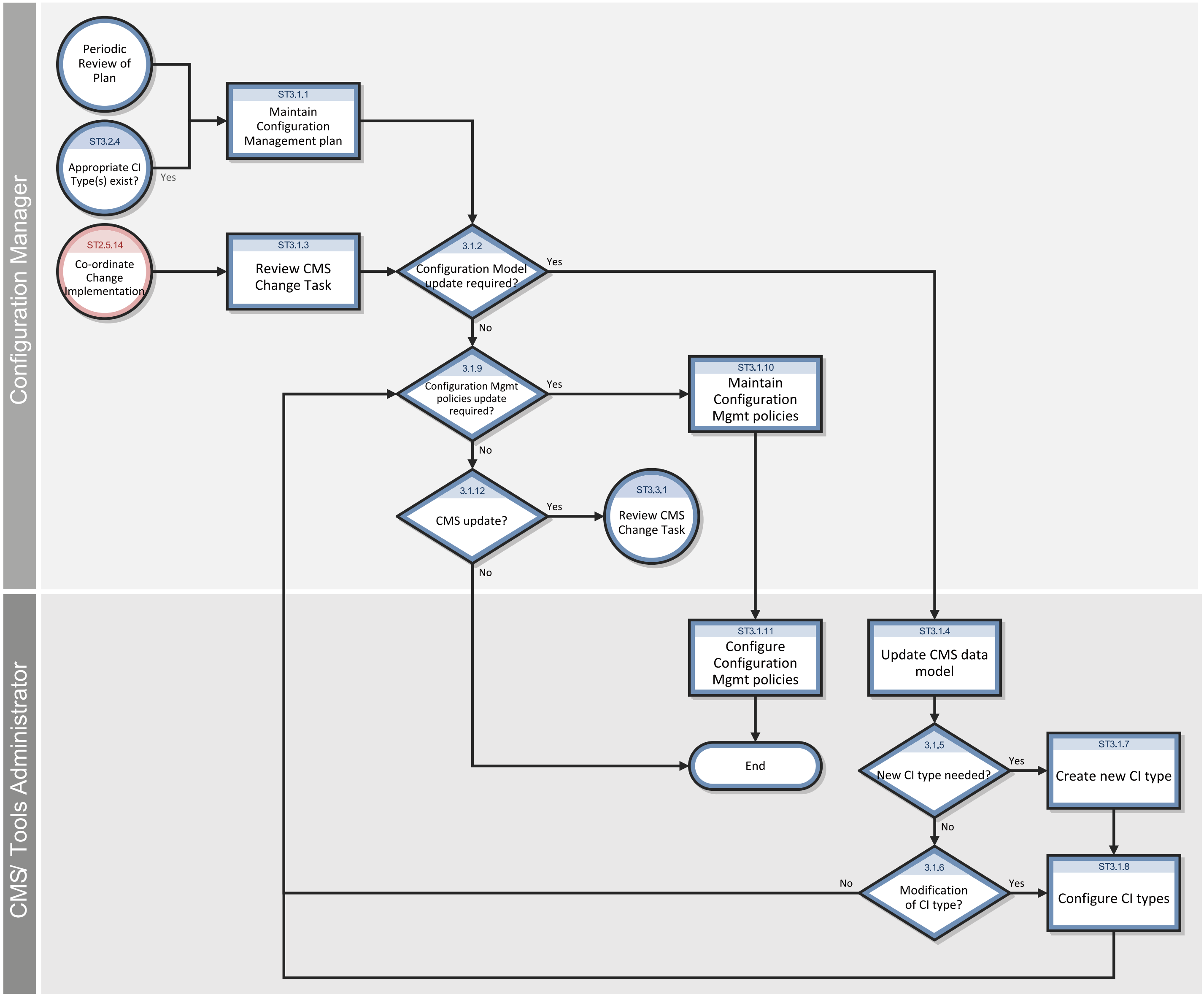
Configuration Management Planning (process ST 3.1)

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

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

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

The Configuration Management Planning workflow is illustrated in the following figure:


Configuration Manager
CMS/ Tools Administrator
Periodic Review of Plan
ST3.2.4
Appropriate CI Type(s) exist?
Yes
ST2.5.14
Co-ordinate Change Implementation
ST3.1.1
Maintain Configuration Management plan
ST3.1.3
Review CMS Change Task
3.1.2
Configuration Model update required?
Yes
No
3.1.9
Configuration Mgmt policies update required?
Yes
No
ST3.1.10
Maintain Configuration Mgmt policies
3.1.12
CMS update?
Yes
No
ST3.3.1
Review CMS Change Task
ST3.1.11
Configure Configuration Mgmt policies
End
ST3.1.4
Update CMS data model
3.1.5
New CI type needed?
Yes
No
ST3.1.7
Create new CI type
3.1.6
Modification of CI type?
No
Yes
ST3.1.8
Configure CI types

Configuration Management Planning process

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

Configuration Management Planning process, continued

Process ID	Procedure or Decision	Description	Role
	of CI type required?		Administrator
ST 3.1.7	Create new CI type	The CMS/Tools Administrator adds a new CI type (device type). This includes the definition of CI attributes and screen design.	CMS/Tools Administrator
ST 3.1.8	Configure CI types	Create or modify the definition of the CI type. This includes: • CI subtypes • Attribute definitions • Screen design • CI relationships types • Naming conventions • Business rules on required fields	CMS/Tools Administrator
ST 3.1.9	Configuration Management policies update required?	The Configuration Administrator determines whether the Configuration Management policies must be updated (to reflect the SCAM plan). If so, go to ST 3.1.12.	Configuration Manager
ST 3.1.10	Maintain Configuration Management policies	The Configuration Manager maintains the Configuration Management policies. Policies may be applicable for specific asset types (or CI Types) or services. Policies may include business rules and requirements for specific information to be maintained in the CMS (for example, for compliance purposes or to monitor contracts). Policies determine how often a configuration audit is required. Policies also designate which data in a CI may be updated by inventory tools, as well as what actions must be performed if unauthorized software is detected. Other items covered by policies and business rules include:	Configuration Manager

Configuration Management Planning process, continued

Process ID	Procedure or Decision	Description	Role
		• Naming conventions • Labeling rules • Asset capitalization rules (for example, to set the depreciation start date) • Procedures for lost or stolen items	
ST 3.1.11	Configure Configuration Management policies	Configuration Management policies and requirements are translated into tool settings (for example, required fields, schedule for automated inventory and discovery, and reconciliation rules).	CMS/Tools Administrator
ST 3.1.12	CMS update?	If yes, go to ST 3.3.1. If not, the process is finished.	Configuration Manager

Configuration Identification (process ST 3.2)

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

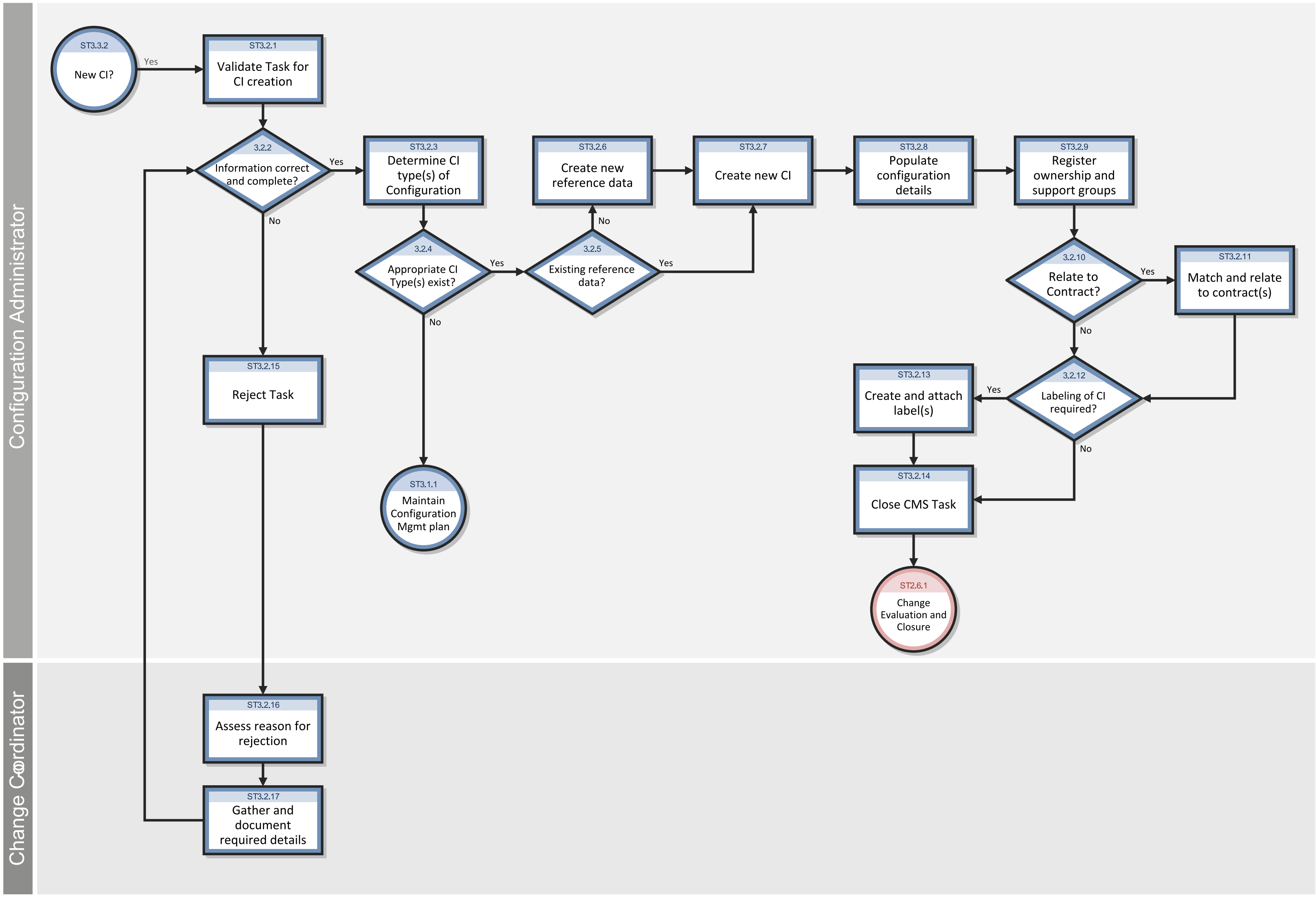
Configuration Identification process is enables you to do the following:

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

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

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

The Configuration Identification workflow is illustrated in the following figure:


Configuration Administrator
Change Coordinator
ST3.3.2
New CI?
Yes
ST3.2.1
Validate Task for CI creation
3.2.2
Information correct and complete?
Yes
No
ST3.2.3
Determine CI type(s) of Configuration
3.2.4
Appropriate CI Type(s) exist?
Yes
No
ST3.2.6
Create new reference data
3.2.5
Existing reference data?
Yes
No
ST3.2.7
Create new CI
ST3.2.8
Populate configuration details
ST3.2.9
Register ownership and support groups
3.2.10
Relate to Contract?
Yes
No
ST3.2.11
Match and relate to contract(s)
3.2.12
Labeling of CI required?
Yes
No
ST3.2.13
Create and attach label(s)
ST3.2.14
Close CMS Task
ST2.6.1
Change Evaluation and Closure
ST3.1.1
Maintain Configuration Mgmt plan
ST3.2.15
Reject Task
ST3.2.16
Assess reason for rejection
ST3.2.17
Gather and document required details

Configuration Identification process

Process ID	Procedure or Decision	Description	Role
ST 3.2.1	Validate task for CI creation	The Configuration Administrator reviews the task to verify that all required information to create a new configuration item is complete and correct. Configuration describes a group of CIs that work together to deliver an IT Service, or a recognizable part of an IT Service. The term configuration can also refer to the parameter settings for one or more CIs.	Configuration Administrator
ST 3.2.2	Information correct and complete?	If the information is correct and complete, continue with ST 3.2.3. If not, go to ST 3.2.15 (reject task).	Configuration Administrator
ST 3.2.3	Determine CI type(s) of configuration	Determine the CI type(s) needed to register the CIs. A CI type is used as a template to document the CI, including, attributes and required fields.	Configuration Administrator
ST 3.2.4	Appropriate CI type(s) exist?	A CI can only be registered if the CI type is known and a Configuration Management policy is available for these types. Existing types must match the attributes that need to be managed and allow designation of a person who is responsible for maintaining the CI. CIs of a registered type can be used as templates for new CIs. If there are existing CI types, continue with ST 3.2.5. If not, go to ST 3.2.11.	Configuration Administrator
ST 3.2.5	Existing reference data?	Verify that the reference data (the product definition from the manufacturer or supplier) for the configuration exist. If there is no reference data, go to ST 3.2.6. If yes, continue with ST 3.2.7.	Configuration Administrator
ST 3.2.6	Create new reference data	Create a reference data.	Configuration Administrator
ST 3.2.7	Create new CI	Create the CIs part of the configuration. One or more CIs can be created. Select the CI type (template). Select the model.	Configuration Administrator
ST 3.2.8	Populate configuration	Enter the required CI attributes, according to the Configuration Management policies. Capture relationships and dependencies between the CIs. Depending upon the CI type and business rules,	Configuration Administrator

Configuration Identification process, continued

Process ID	Procedure or Decision	Description	Role
	details	examples of details include: • Serial number location (for example, on stock) • Purchase order number • Receipt date warranty conditions and warranty end date • CI specific attributes	
ST 3.2.9	Register ownership and support groups	All CIs must be assigned to an owner (that is, a reference to an organizational entity such as a cost center) and an administrator (the group responsible for managing the CI during its life cycle). Activities include: • Assign owner • Assign Configuration Administrator (group) • Assign support group for incident assignment (for example, if needed for automated assignment in case of events detected on the device)	Configuration Administrator
ST 3.2.10	Relate to contract?	Determine related contracts for the components, such as: • Maintenance or support contracts • Financial contracts (for example, lease or rental) • License contract or service contracts (for example, SLA, UC, and OLA) If no contracts are relevant for this Configuration, go to ST 3.2.12. If yes, continue with ST 3.2.11 to link the items to the contract.	Configuration Administrator
ST 3.2.11	Match and relate to	Link the CIs to one or more contracts. Capture the inclusion date of the CI to the contract. If needed, inform the Contract Manager of the new items attached to the contract.	Configuration Administrator

Configuration Identification process, continued

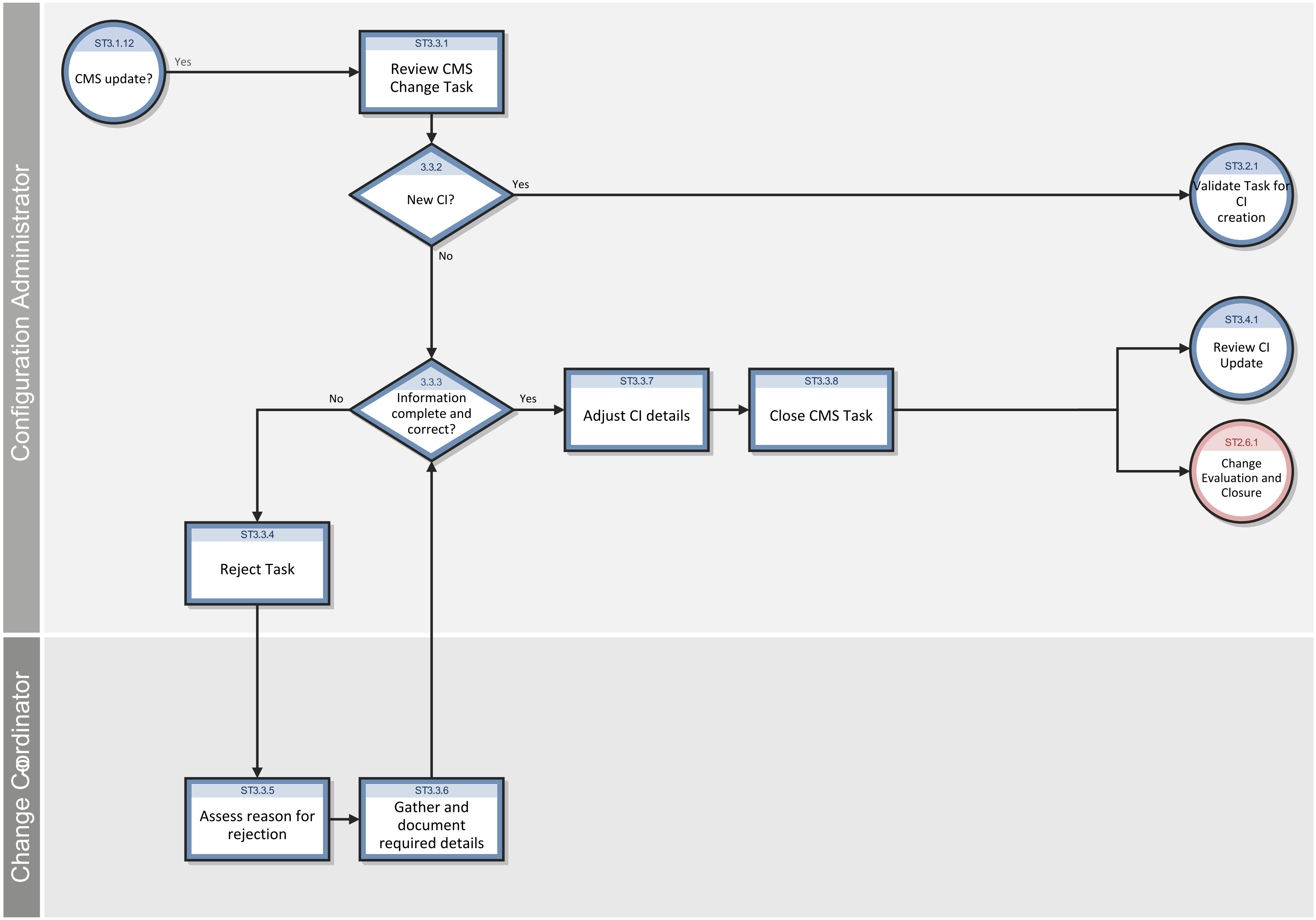
Process ID	Procedure or Decision	Description	Role
	contract(s)		
ST 3.2.12	Labeling of CI required?	Determine whether CIs need to be labeled according to the Configuration Management policies. If not, go to ST 3.2.14. If yes, continue with ST 3.2.13.	Configuration Administrator
ST 3.2.13	Create and attach label	Create and print a label. Physically attach the label to the CI.	Configuration Administrator
ST 3.2.14	Close Configuration Management task	After completion, the task can be closed. Update closure code.	Configuration Administrator
ST 3.2.15	Reject task	If the task cannot be completed, reject the task. Update the task with reasons and details of any issues found.	Configuration Administrator
ST 3.2.16	Assess reason for rejection	The Change Coordinator assesses the reason for the rejection.	Change Coordinator
ST 3.2.17	Gather and document required details	The Change Coordinator documents the details related to the rejected task.	Change Coordinator

Configuration Control (process ST 3.3)

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

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

The Configuration Control workflow is illustrated in the following figure:


Configuration Administrator
Change Coordinator
ST3.1.12
CMS update?
Yes
ST3.3.1
Review CMS Change Task
3.3.2
New CI?
Yes
No
ST3.2.1
Validate Task for CI creation
ST3.4.1
Review CI Update
3.3.3
Information complete and correct?
No
Yes
ST3.3.7
Adjust CI details
ST3.3.8
Close CMS Task
ST2.6.1
Change Evaluation and Closure
ST3.3.4
Reject Task
ST3.3.5
Assess reason for rejection
ST3.3.6
Gather and document required details

Configuration Control process

Process ID	Procedure or Decision	Description	Role
ST 3.3.1	Review CMS Change task	The Configuration Administrator reviews the task for updating the Configuration Management System (CMS).	Configuration Administrator
ST 3.3.2	New CI?	If the task refers to the creation of one or more new CIs, go to ST 3.2.1 and follow the procedure to validate a task for CI creation. If the task is related to the modification of an existing CI, continue with ST 3.3.3.	Configuration Administrator
ST 3.3.3	Information complete and correct?	Verify that all information to update the CIs is available and correct. The task should refer to at least one CI that must be updated. The task contains a description of the attributes to be modified. If not all information is complete and correct, go to ST 3.3.4 (reject task). If yes, continue with ST 3.3.7.	Configuration Administrator
ST 3.3.4	Reject task	If the configuration update cannot be completed, the task is rejected. A reason and recommended actions must be provided.	Configuration Administrator
ST 3.3.5	Assess reason for rejection	The Change Coordinator assesses the reason for the rejection.	Change Coordinator
ST 3.3.6	Gather and document required details	The Change Coordinator documents the details related to the rejected task.	Change Coordinator
ST 3.3.7	Adjust CI details	Modify the configuration details in the Configuration Management database. Configuration modifications can include: • Status (items transferred from test to production or to retirement) • Location (moves) • Relationships and dependencies	Configuration Administrator

Configuration Control process, continued

Process ID	Procedure or Decision	Description	Role
		• Installation of software on the item • Transfer of ownership • Assign contract to a CI	
ST 3.3.8	Close CMS task	After completion of the configuration updates, the task can be closed.	Configuration Administrator

Configuration Status Accounting and Reporting (process ST 3.4)

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

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

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

- Lost or stolen items
- Unauthorized CIs and Version changes of CIs

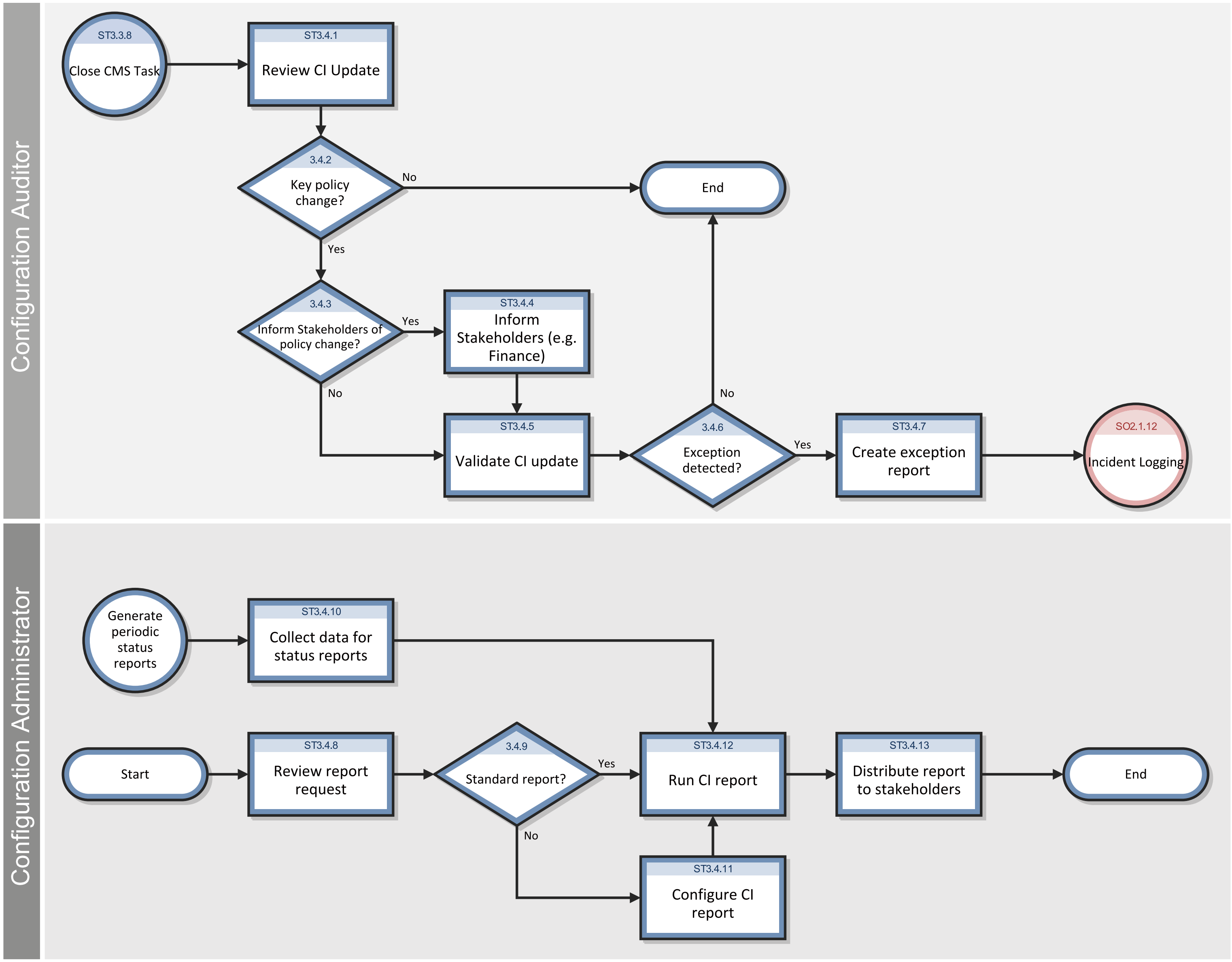
Current and accurate configuration records should be maintained to reflect changes in the status, location, and versions of CIs. The history of each CI must be maintained. Changes to CIs are tracked through various states, such as ordered, received, in acceptance test, live, under change, withdrawn,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

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

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

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

The Configuration Status Accounting and Reporting workflow is illustrated in the following figure:


Configuration Auditor
ST3.3.8
Close CMS Task
ST3.4.1
Review CI Update
3.4.2
Key policy change?
No
End
Yes
3.4.3
Inform Stakeholders of policy change?
Yes
ST3.4.4
Inform Stakeholders (e.g. Finance)
No
ST3.4.5
Validate CI update
3.4.6
Exception detected?
No
Yes
ST3.4.7
Create exception report
SO2.1.12
Incident Logging
Configuration Administrator
Generate periodic status reports
ST3.4.10
Collect data for status reports
Start
ST3.4.8
Review report request
3.4.9
Standard report?
Yes
No
ST3.4.12
Run CI report
ST3.4.11
Configure CI report
ST3.4.13
Distribute report to stakeholders
End

Configuration Status Accounting and Reporting process

Process ID	Procedure or Decision	Description	Role
ST 3.4.1	Review CI update	Modifications of key attributes of the CI are logged in the history log and verified. During Configuration Identification and control activities, configuration status records are created. These records enable key changes to be visible and traceable. CI attributes that can be logged include: • status (for example, system down) • version number • serial number • installation date • audit status (for example, missing or lost) • removed from a contract Critical CI changes are logged with entries for reason, date stamp, time stamp, and person recording the status change.	Configuration Auditor
ST 3.4.2	Key policy change?	Determine whether the policy must be reviewed or validated, based on the documented Configuration Management policies (and policies related to finance, procurement, Contract Management, and security).	Configuration Auditor
ST 3.4.3	Inform stakeholders of policy change?	Specific changes must be reported to the stakeholders. These include: • Procurement • Finance (for example, by linking to the general ledger) • Contract Manager Verify that the event must be reported. If not, go to ST 3.4.5. If yes, continue with ST 3.4.4.	Configuration Auditor

Configuration Status Accounting and Reporting process, continued

Process ID	Procedure or Decision	Description	Role
ST 3.4.4	Inform stakeholders	Inform stakeholders of the event (for example, the Contract Manager when an asset is included in the contract, or procurement when an item is received). Examples of events that should trigger stakeholder notification include: • Received and accepted items • Installation of the asset (for example, for depreciation start date) • Lost or stolen item • Retirement or disposal of an item (for finance)	Configuration Auditor
ST 3.4.5	Validate CI update	Confirm that all relevant status data documented in the CI is complete and correct, according to Configuration Management policies derived from agreements, relevant legislation, and standards. Ensure that the status change or version update is a result of an authorized change.	Configuration Auditor
ST 3.4.6	Exception detected?	If the CI update or CI details are not correct or complete according to the Configuration policies, continue with SO3.4.7.	Configuration Auditor
ST 3.4.7	Create exception report	Create a new incident (see SO 2.1.11).	Configuration Auditor
ST 3.4.8	Review report request	The Configuration Administrator reviews the request for Configuration Management information.	Configuration Administrator
ST 3.4.9	Standard report?	Configuration Management has defined a number of standard reports (for example, overview of CIs in stock or by status). If this is a standard report, continue with ST 3.4.12. If not, go to ST 3.4.11.	Configuration Administrator
ST 3.4.10	Collect data for status reports	Periodically, Configuration Management procedures provide reports for the different stakeholders, such as financial asset managers, contract managers, or procurement.	Configuration Administrator

Configuration Status Accounting and Reporting process, continued

Process ID	Procedure or Decision	Description	Role
ST 3.4.11	Configure CI report	If a standard report does not exist, the Configuration Administrator creates a query to select the data to display from the CMS.	Configuration Administrator
ST 3.4.12	Run CI report	The report or query is run against the database. The data is collected in a standard format.	Configuration Administrator
ST 3.4.13	Distribute report to stakeholders	Provide the requested data to the stakeholders. Close the request (if applicable).	Configuration Administrator

Configuration Verification and Audit (process ST 3.5)

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

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

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

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

Configuration Verification and Audit activities include:

- Make sure that baselines and standards match the actual components in the IT environment
- Verify that services and products are built and documented, according to documented requirements, standards, or contractual agreements
- Verify that the correct and authorized versions of any CI exists and is correctly identified and described
- Verify the physical existence of CIs (for example, in the organization, in the Definitive Media Library, or in stock)
- Check that release documentation and configuration administration are present before making a release
- Confirm that the current environment is as expected and documented in the CMS, and that any Change requests are resolved
- Check that configuration modifications are implemented through authorized changes
- Validate the existence of a SLA against each CI
- Verify that CI specifications are compliant with defined configuration policies and baselines
- Validate that all required documentation for each CI is available (for example, maintenance contracts, license records, or warranties)
- Check data quality for accuracy and completeness
- Initiate an incident for discovered unauthorized changes

The following are examples of discrepancies:

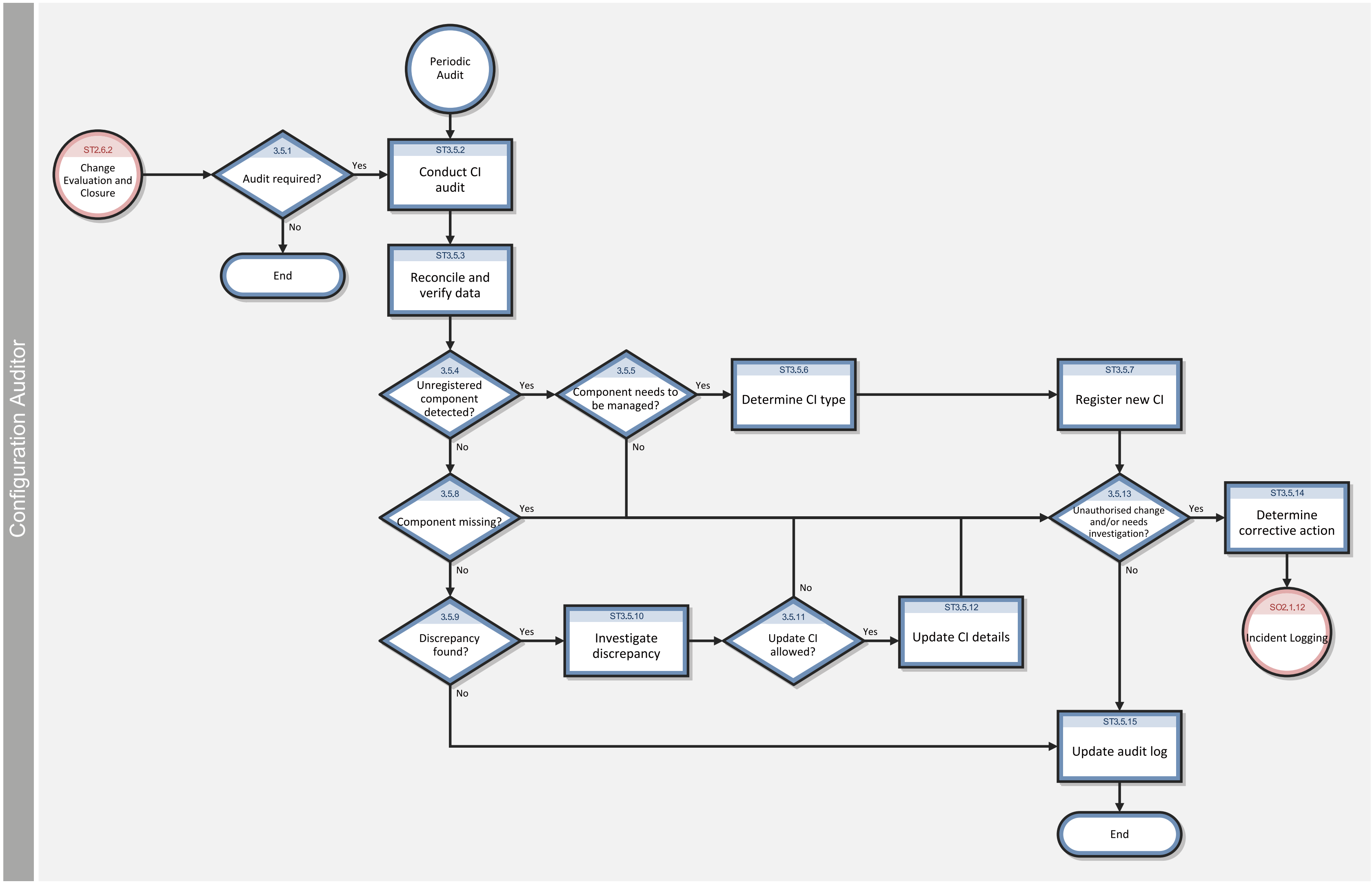
- Unauthorized software installed
- Unauthorized access to resources and services (for example, access rights not reflected in subscriptions)
- Discrepancy of status or configuration details, as registered in the CMS, compared with the actual status.

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

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

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

The Configuration Verification and Audit workflow is illustrated in the following figure:



Configuration Verification and Audit process

Process ID	Procedure or Decision	Description	Role
ST 3.5.1	Audit required?	Configuration audits should be considered before and after a major change or release.	Configuration Auditor
ST 3.5.2	Conduct CI audit	Configuration audits (manual or automated) are scheduled periodically. The audit verifies each individual CI. It uses an automated inventory tool that scans the system. Another method is to scan the IT environment and discover the component connected to the enterprise. New components may be discovered, requiring management in the CMS.	Configuration Auditor
ST 3.5.3	Reconcile and verify data	Collected data from the audit must be reconciled and compared with the data already stored in the CMS. Different reconciliation keys and rules can be applied to match the discovered item with the CI in the CMS.	Configuration Auditor
ST 3.5.4	Unregistered component detected?	An unregistered component may be detected in cases where the item cannot be matched and found in the CMS. If an unregistered component is detected, go to ST 3.5.5. If not, continue with ST 3.5.8.	Configuration Auditor
ST 3.5.5	Component needs to be managed?	Determine whether the new component needs to be registered in the CMS, based on the scope of the CMS. If yes, continue with ST 3.5.6. If no, go to ST 3.5.13.	Configuration Auditor
ST 3.5.6	Determine CI type	The CI type is selected, based on the properties of the discovered component (for example, model name or type of device).	Configuration Auditor
ST 3.5.7	Register new CI	Create a new CI. Enter the additional attributes of the CI, based on the audit data. Go to ST 3.5.13.	Configuration Auditor
ST 3.5.8	Component missing?	If a component cannot be discovered during an audit, it may be lost or stolen (for example, the CI has not been connected to the network for some period of time). The audit status is updated to Lost. If yes, continue with ST 3.5.13. If no, continue with ST 3.5.9.	Configuration Auditor
ST 3.5.9	Discrepancy found?	Based upon the comparison between the CMS administration and the actual data from the audit, one or more discrepancies may be detected. If yes, continue with ST 3.5.10. If not, continue with ST 3.5.15.	Configuration Auditor

Configuration Verification and Audit process, continued

Process ID	Procedure or Decision	Description	Role
ST 3.5.10	Investigate discrepancy	The mismatch between the CMS administration and the actual configuration is investigated in more detail. For each discrepancy, attribute differences and relationships are investigated.	Configuration Auditor
ST 3.5.11	Update CI allowed?	To reduce the number of manual activities, some fields are populated by discovery and auditing tools. These attributes will not be maintained manually. Determine whether the differences can be updated directly without a formal change procedure. If yes, continue with ST 3.6.12. If no, go to ST 3.5.13.	Configuration Auditor
ST 3.5.12	Update CI details	The configuration details are updated, based on the audit date to ensure that the administration is correctly reflecting the actual situation.	Configuration Auditor
ST 3.5.13	Unauthorized change and/or needs investigation?	Determine whether the mismatch between the audit and the CMS administration requires further investigation (for example, detection of unauthorized software). If yes, go to ST 3.5.14. If no, continue with ST 3.5.15.	Configuration Auditor
ST 3.5.14	Determine corrective action	Document the discrepancy and determine the appropriate actions (for example, additional investigation is needed). An incident must be created and assigned to the person responsible for executing the actions. Follow SO 2.1.11 to create a new incident.	Configuration Auditor
ST 3.5.15	Update audit log	The CI is updated with the audit status and last audit date.	Configuration Auditor

Master data management (process ST 3.6)

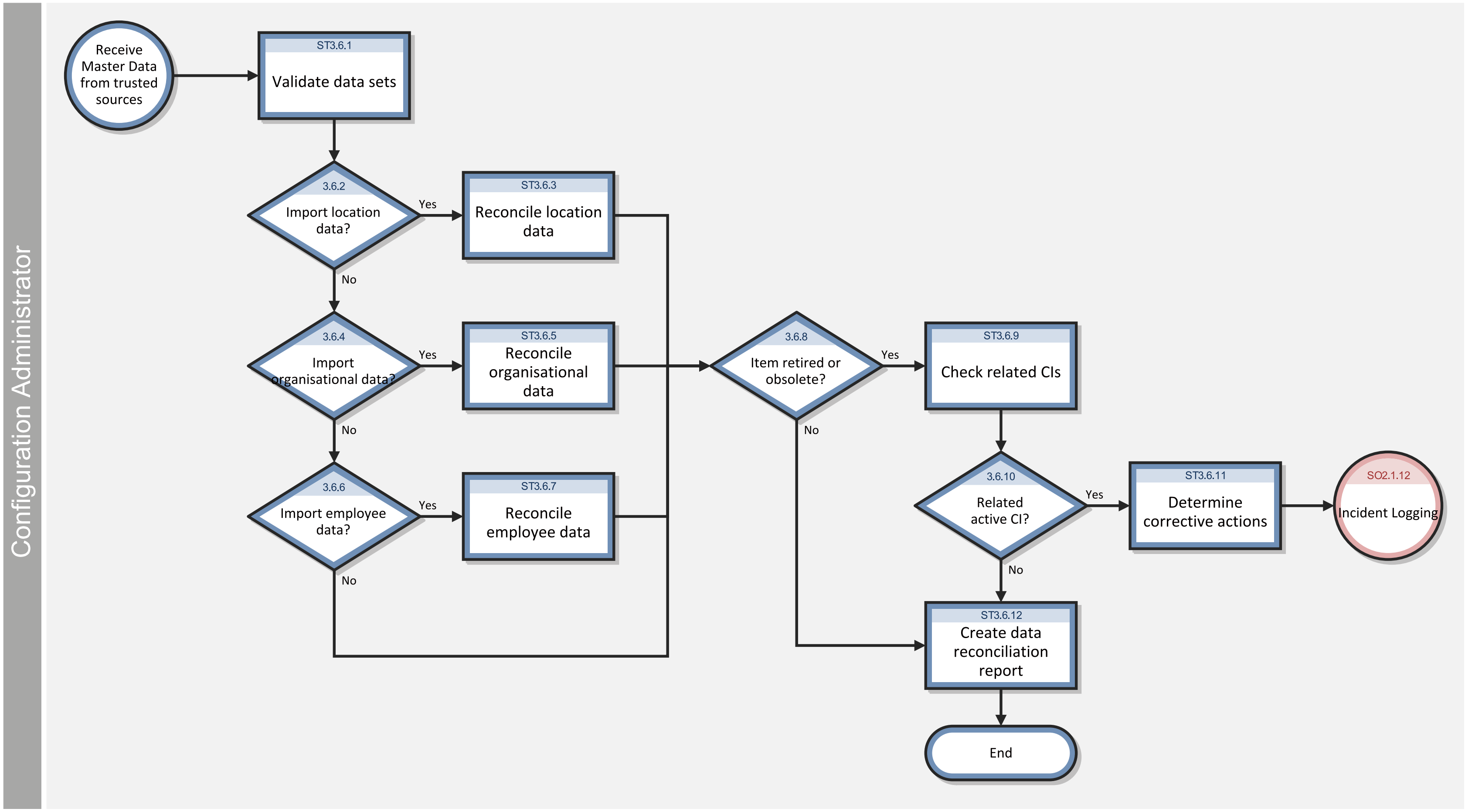
Master reference data is key data that the Configuration Management System (CMS) depends on and is often provided by different organizational functions, such as human resources management, finance, and facilities. For example, master data can include details about organization units, cost centers, employee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

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

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

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

Master data management workflows is illustrated in the following figure:



Master data management process

Process ID	Procedure or Decision	Description	Role
ST 3.6.1	Validate data sets	Periodically data sets are received from trusted sources. The Configuration Administrator checks the format and content against the defined specifications.	System Administrator Configuration Administrator
ST 3.6.2	Import location data?	If you want to import location data, continue with ST 3.6.3. If not, go to ST 3.6.4.	System Administrator Configuration Administrator
ST 3.6.3	Reconcile location data	Import and load location data into the CMS.	System Administrator Configuration Administrator
ST 3.6.4	Import organizational data?	If you want to import organizational data, continue with ST 3.6.5. If not, go to ST 3.6.6.	System Administrator Configuration Administrator
ST 3.6.5	Reconcile organizational data	Import and load organizational data into the CMS.	System Administrator Configuration Administrator
ST 3.6.6	Import employee data?	If you want to import employee data, continue with ST 3.6.7. If not, stop.	System Administrator Configuration Administrator

Master data management process, continued

Process ID	Procedure or Decision	Description	Role
ST 3.6.7	Reconcile employee data	Import and load employee data into the CMS.	System Administrator Configuration Administrator
ST 3.6.8	Item retired or obsolete?	Verify that one or more items in the data set are retired or no longer present. Make sure to update the status of items in the CMS.	System Administrator Configuration Administrator
ST 3.6.9	Check related CIs	Verify that one or more CIs are still related to retired items in the modified master data record. For example, a retired user may still have one or more subscriptions or CIs for which that user is responsible. Updates of interest include: • Status updates (for example, retirement) • Job profile changes (for validating access rights and related current subscriptions) • Reorganizations (for example, merge or split of departments) • Cost center changes Master data modifications must be verified to ensure that these updates do not conflict with configuration administration.	System Administrator Configuration Administrator
ST 3.6.10	Related active CI?	If there is a related active CI, continue with ST 3.6.11. If not, go to ST 3.6.12.	System Administrator Configuration Administrator
ST	Determine	Follow the procedure to create a new incident (see SO 2.1.11).	System

Master data management process, continued

Process ID	Procedure or Decision	Description	Role
3.6.11	corrective actions		Administrator Configuration Administrator
ST 3.6.12	Create data reconciliation report	Create a report with a summary of data modifications and reconciliation errors, which includes statistics of the number of modifications (for example, new items and retired items).	System Administrator Configuration Administrator

Chapter 18: Configuration Management Details

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

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

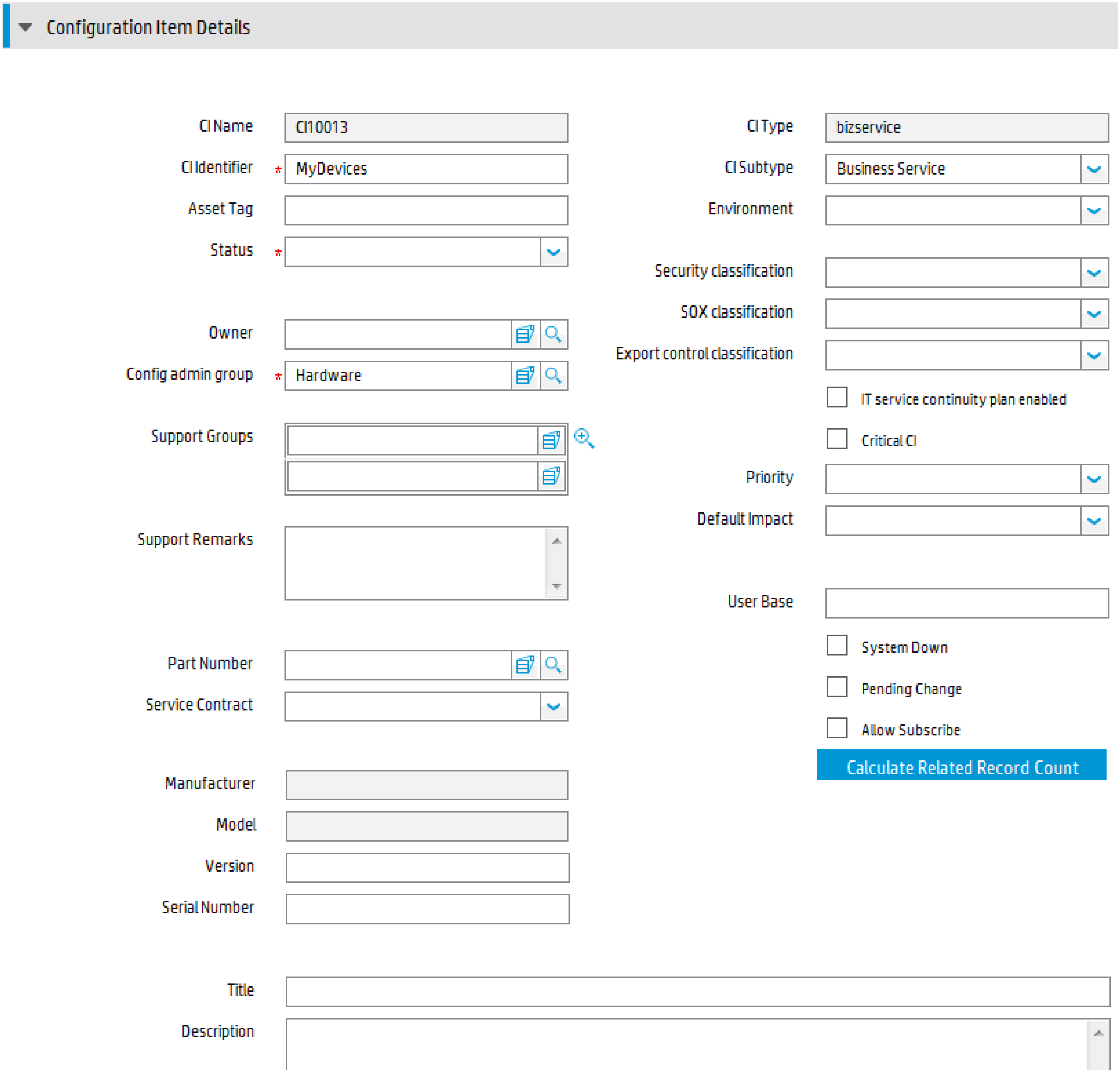
Topics in this section include:

- "MyDevices configuration item form" below
- "Configuration Management form details" on the next page

MyDevices configuration item form

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

The MyDevices configuration item form is illustrated in the following screenshot:



Configuration Item Details

CI Name: CI10013

CI Identifier *: MyDevices

Asset Tag:

Status *:

Owner:

Config admin group *: Hardware

Support Groups:

Support Remarks:

Part Number:

Service Contract:

Manufacturer:

Model:

Version:

Serial Number:

CI Type: bizservice

CI Subtype: Business Service

Environment:

Security classification:

SOX classification:

Export control classification:

□ IT service continuity plan enabled

□ Critical CI

Priority:

Default Impact:

User Base:

□ System Down

□ Pending Change

□ Allow Subscribe

Title:

Description:

Configuration Management form details

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

Configuration Management field descriptions

Label	Description
CI Identifier	The name of the CI. This is a required field.
CI Name	System-generated field that specifies the unique ID of the configuration item (CI).
Asset Tag	This is a legacy field intended for customers migrating from previous versions of

Configuration Management field descriptions, continued

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

Configuration Management field descriptions, continued

Label	Description
	uniquely identify the CI.
Model	This is a system-generated field that specifies the manufacturer’s model if one is associated with the Part Number. This field along with manufacturer and serial number uniquely identify the item.
Version	This field specifies the manufacturer’s version number for the CI.
Serial Number	This field specifies the manufacturer’s serial number for the CI.
Title	This field specifies the title of the CI owner; for example Mr. or Mrs.
Description	This field is a free-form text field to add additional information about the CI.
CI Type	This field identifies the type of CI. The out-of-box data is: • Application • Business Service • CI Group • Computer • Display Device • Example • Furnishings • Hand Held Devices • Mainframe • Network Components • Office Electronics • Software License • Storage • Telecommunications The Managed State section displays different fields depending on the CI type selected.
CI Subtype	This field identifies the subtype of CI. The list of available subtypes depends upon the CI Type the user selected. For more information, see the "Configuration Item types and subtypes" on page 286 table.

Configuration Management field descriptions, continued

Label	Description
Environment	This field specifies if a CI belongs to a particular environment. The out-of-box data is: • Development • Test • Production • Failover • None
Security classification	This field specifies if the CI has any security restrictions. The out-of-box data is: • Unrestricted • Restricted • Confidential • Most Confidential
SOX classification	This field specifies if the CI has a Sarbanes Oxley (SOX) classification that applies to the CI. The out-of-box data is: • Critical • Non Critical
Export control classification	This field specifies if the CI has an Export Control classification. The out-of-box data is: • EAR99 (Non Controlled) • 4D994 • 5D991 • 5D002 • 5D992
IT service continuity plan enabled	This field specifies if the CI has an IT service continuity plan enabled for it.
Critical CI	This field specifies if the CI is critical for day-to-day operation, such as an E-mail server or RDBMS server. If you open an incident on a critical CI, the incident indicates that this is a critical CI.

Configuration Management field descriptions, continued

Label	Description
Priority	This field specifies the default priority of any related records opened against the CI. The information in this field is used to prepopulate the priority in an incident or interaction. When a user selects the CI in an incident or interaction, it populates the incident or interaction priority based on the CI priority field. The out-of-box data is: • 1 - Critical • 2 - High • 3 - Average • 4 - Low For additional information, see the "Incident Management form details" on page 97 table.
Default Impact	This field specifies the default impact of any related record opened against the CI. The information in this field is used to prepopulate the impact in an incident or interaction. When a user selects the CI in an incident or the interaction, it populates the incident or interaction impact based on the CI Default Impact field. The out-of-box data is: • 1 - Enterprise • 2 - Site/Dept • 3 - Multiple Users • 4 - User For additional information, see the "Incident Management form details" on page 97 table.
Calculate Related Record Counts	Clicking this button displays a count of related incidents, problems, known errors, and changes that were opened against this CI.
User Base	This field displays a count of the number of users who use the CI.
System Down	This field indicates whether the CI is currently operational or has an open incident related to it causing it to be non-operational. When you close the incident for the CI, this action clears the flag. The CI is no longer marked as down.
Pending Change	This field indicates whether or not there are any changes pending against this CI. When you close or open a change for the CI, this action sets or clears the flag.
Allow Subscribe	This field determines if the CI is available for subscriptions from the Service Catalog.

Configuration Management field descriptions, continued

Label	Description
Baseline > Baseline	This field indicates if the CI has an associated baseline and if the CI is in compliance.
Baseline > Baseline Version	This field indicates the baseline version that the CI is tracked against. Baseline Versions enable you to have CIs with the same baseline configuration but slight differences. You can have several versions of that baseline, or if you have updates for a new version of a software installed, then you can select a specific version of a baseline for a CI.
Managed State	This section lists the expected values of CI attributes. All changes to fields in the Managed State section require a Change Management record. See the "Managed State subsections" on page 289 table for the Managed State subsection field descriptions.
Actual State	This section lists the actual values of CI attributes if the Service Manager system has an integration to HP Universal CMDB. It shows the latest discovered information from the UCMDB or its sources.
CI Changes > Pending Attribute Changes	This field lists the attributes that are waiting to be changed through a Change Management record or changes requested through an Unplanned Change (requires an HP Universal CMDB integration). The data in this field can only be modified through Change Management. Each CI has a set of managed attributes that can be changed through Change Management.
CI Changes > Historic Attribute Changes	This field lists the attributes that are have already been changed through a Change Management record or changes requested through an Unplanned Change (requires an HP Universal CMDB integration).
Relationships > Upstream Relationships > Upstream Configuration Item, Relationship Name, Relationship Type, Relationship Subtype	This field shows information about which upstream CIs are dependent on the selected CI. Upstream CIs depend on the current CI. For example, the upstream E-mail service depends on the downstream E-mail server, the network, and your E-mail program.
Relationships > Upstream Relationships > Add	This option links to the add a new CI relationship record that enables you to add a new upstream relationship to this CI.
Relationships > Upstream	This option provides different views of upstream CI relationships for the specified CI.

Configuration Management field descriptions, continued

Label	Description
Relationships > View Relationship Type (All, Logical, Physical)	• All: displays all upstream CI relationships for this CI that are either physical or logical. • Logical: displays all upstream logical CI relationships for the specified CI. A logical connection means that you can access the CI but there is no direct physical connections to other CIs. For example, a network printer that you use. • Physical: displays all upstream physical CI relationships for the specified CI. A physical connection is when a CI is directly attached to another device. For example, a PC connected to a dedicated printer with printer cable. To view ALL/Logical/Physical upstream relationships of the specified CI, select an option in the View Relationship Type field and then click **Filter**. A list of CI relationship records displays. Click **Cancel** in a CI relationship record to return to the specified CI.
Relationships > Downstream Relationships > Relationship Name, Relationship Type, Relationship Subtype	This option shows the CIs that have a downstream dependency on this CI. For example, the upstream E-mail service depends on the downstream E-mail server, the network, and your E-mail program.
Relationships > Downstream Relationships > Add	This option links to the add a new CI relationship record that enables you to add a new downstream relationship to this CI.
Relationships > Downstream Relationships > View Relationship Type (All, Logical, Physical)	This option provides different views of downstream CI relationships for the specified CI. • All: displays all downstream CI relationships for this CI that are either physical or logical. • Logical: displays all downstream logical CI relationships for the specified CI. A logical connection means that you can access the CI but there is no direct physical connections to other CIs. For example, a network printer that you use. • Physical: displays all downstream physical CI relationships for the specified CI. A physical connection is when a CI is directly attached to another device. For example, a PC connected to a dedicated printer with printer cable. To view ALL/Logical/Physical downstream relationships of the specified CI, select an option in the View Relationship Type field and then click **Filter**. A list of CI relationship records displays. Click **Cancel** in a CI relationship record to return to

Configuration Management field descriptions, continued

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

Configuration Management field descriptions, continued

Label	Description
Objectives, Max Duration Objectives	
Financial > Contracts, Expense Lines, Labor, Parts	This section displays information for the service contracts, parts, labor, and expenses for the CI.
Attachments	This section displays the Filename and Size of each attachment of the CI record. Users can add new attachments using the **Add File** button and remove any existing attachments by clicking the remove links.

Configuration Item types and subtypes

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

Configuration Item types and subtypes

CI Name	CI Type	CI Subtype
Application	application	Anti-Virus / Security Back-up Business Development Tools Entertainment Graphics Internet/Web Networking Operating System Reference Other
Business Service	bizservice	Business Service Application Service Infrastructure Service
CI Group	cigroup	Ad Hoc Baseline
Computer	computer	Desktop Dumb Terminal Laptop Tower

Configuration Item types and subtypes, continued

CI Name	CI Type	CI Subtype
		MAC Server Host VAX Windows Unix Mainframe Logical Partition Terminal Server
Display Device	displaydevice	Monitor Projector
Example	example	
Furnishings	furnishings	Artwork Armoire Bookcase Chair Computer Desk Desk Collection File Cabinet Meeting Table
Hand Held Devices	handhelds	PDA Cell Phone Pager Blackberry Device GPS Device
Mainframe	mainframe	Controller Host CPU FEP NCP LPAR
Network Components	networkcomponents	Router Hub Switch Modem Network Interface Card Gateway Firewall Network Component ATM Switch RAS LB Concentrator

Configuration Item types and subtypes, continued

CI Name	CI Type	CI Subtype
		Net Device Switch Router
Office Electronics	officeelectronics	Copy Machine Printer Fax Machine Paper Shredder Camera Speaker Calculator Multifunction Word Processor Typewriter VCR Television UPS Net Printer
Software License	softwarelicense	DBMS License Development Tool License Enterprise Management License Operating System License Outlook Productivity Tools License Project Management License Utility Software License
Storage	storage	CDRW Direct Attached Storage (DAS) HDD Network Attached Storage (NAS) Storage Area Network (SAN) ZIP CD Burner
Telecommunications	telcom	Desk Phone Flush Wall Mount Headsets & Accessories NBX PBX Paging Solution Surface Mount

Managed State subsections

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

The following table outlines the subsections and fields available for the different CI types.

Managed State subsections

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

Managed State subsections, continued

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

Chapter 19: Request Fulfillment Overview

The HP Service Manager Request Fulfillment application, referred to as Request Fulfillment throughout this chapter, supports the Request Fulfillment process. It enables you to route and support all requests for non-standard operational services in an effective way, and ensure that requests will not compromise day-to-day operational activities.

This section describes how Request Fulfillment implements the best practice guidelines for the Request Fulfillment processes.

Topics in this section include:

- "Request Fulfillment within the ITIL framework" below
- "Request Fulfillment application" on the next page
- "Request Fulfillment process overview" on page 296
- "Input and output for Request Fulfillment" on page 300
- "Key performance indicators for Request Fulfillment" on page 300
- "RACI matrix for Request Fulfillment" on page 303

Request Fulfillment within the ITIL framework

Request Fulfillment is addressed in ITIL's *Service Operation* publication. The document describes Request Fulfillment as the process responsible for dealing with Service Requests. Many of these are actually small-sized, low cost, frequently performed, and low-risk, which means they are better handled by a separate process rather than being allowed to congest and obstruct the normal incident and change management processes.

Request Fulfillment enables you to meet the following business objectives:

- Maintain user and customer satisfaction through efficient and professional handling of all service requests.
- Provide a channel for users to request and receive standard services for which a pre-defined authorization and qualification process exists.

- Provide information to users and customers about the availability of services and the procedures for obtaining them.
- Source and deliver the components for requested standard services such as licenses and software media.
- Assist with some general information, complaints or comments.

Request Fulfillment includes the following key features:

- Request model, which defines the prerequisites, required authorizations, and sequenced or parallel standard tasks to fulfill the service request
- A detailed, customizable catalog of products
- Scheduling of service requests and tasks
- Automated request fulfillment
- Order and stock management
- Interaction with other Service Manager applications, such as Service Catalog, Configuration Management, Service Desk, Incident Management, Change Management, and Service Level Management
- Integration with other Service Manager applications, such as Configuration Management and Change Management.
- Integration with other products, including:
  - Providing a common web service interface so that other products are able to access service requests and tasks
  - Integration with Asset Manager for request fulfillment billing

Request Fulfillment application

The HP Service Manager Request Fulfillment is an application used to manage user requests for products and services. Requests affect only the person making the request, or a subordinate group of employees. Examples include password resets, individual PC upgrades, and new employee setup.

The Request Fulfillment application enables business staff to improve their productivity or the quality of business services and products. It can also help reduce the cost of providing services and reduce people effort involved in requesting and receiving access to services. Moreover, the use of Request Fulfillment application can increase the control level of an organization’s services and the number of fulfilled requests.

Request Fulfillment includes the following key features:

- Request model, which defines the prerequisites, required authorizations, and sequenced or parallel standard tasks to fulfill the service request
- A detailed, customizable catalog of products
- Scheduling of service requests and tasks
- Automated request fulfillment
- Order and stock management
- Interaction with other Service Manager applications, such as Service Catalog, Configuration Management, Service Desk, Incident Management, Change Management, and Service Level Management
- Integration with other products, including:
  - Providing a common web service interface so that other products are able to access service requests and tasks
  - Integration with Asset Manager for request fulfillment billing

Differences between Request Fulfillment and Change Management

Request Fulfillment and Change Management are separate processes, but they are closely related. Request Fulfillment handles common user requests for products and services. These requests usually affect only the person making the request, or a subordinate group of employees. Change Management handles any change to your business that modifies or disrupts the current state of that environment. Usually these modifications or disruptions affect multiple users or business units.

- Request Fulfillment
    - Handles common requests for products and services.
    - Affects a small or limited number of users.
    - Scope is limited.
- Change Management
    - Manages changes (implementations) that modify a business environment.
    - Affects many users.
    - Scope is often large, including large groups or multiple business units.

Key elements of Request Fulfillment

Request Fulfillment includes the following key elements.

Request Model

A repeatable model of handling a particular category of service request. A request model defines specific agreed tasks that need to be followed to fulfill the service request of this category. Request models can be very simple, with no requirement for authorization (for example, password reset), or can be complex with many sequential or parallel tasks that require authorization (for example, provision of an existing IT service).

Product Catalog

The product catalog is a predefined catalog of products (hardware, software, or called parts). The product catalog defines the models of independent items that may be requested or ordered.

The product catalog supports general information of parts, including part number, description, cost, and manufacturer. The inventory of the specific item is also available in the product catalog portal. The receiving details of the purchased items can be pre-defined in the product catalog.

Catalog items are represented as records in the `productCatalog` table.

Vendors

Vendors are internal or external providers of parts. Vendors have a many-to-many relationship with catalog items, and may or may not directly interact with Service Manager.

Vendors are represented as records in the `vendor` table. The terms under which a specific vendor will provide a specific catalog item are stored in the `modelvendor` table.

Requests

A request is a high level record that defines the basic request information such as requester, required dates, coordinator, and description. Request records are the "tickets" that trace the workflow of a request from the user perspective, data entry and request task addition, through authorizations, fulfillment, and follow-up.

Request records are stored in the `request` table.

Request Tasks

A request task is a low level record that defines one of the steps to fulfill the service request. Request tasks can be created automatically according to the request model definition or manually by the authorized users. After creation, request tasks are assigned to internal workgroups or external vendors.

Request tasks are stored in the `requestTask` table.

Orders

Order records are the "tickets" that trace the workflow of an actual order of a part item or several part items from the ordering and receiving perspective. Orders are created manually by authorized users or by automated background processes when the reorder rules defined for stock management are satisfied.

Order records are stored in the `request` table, with a particular "Order" category.

Authorization processing

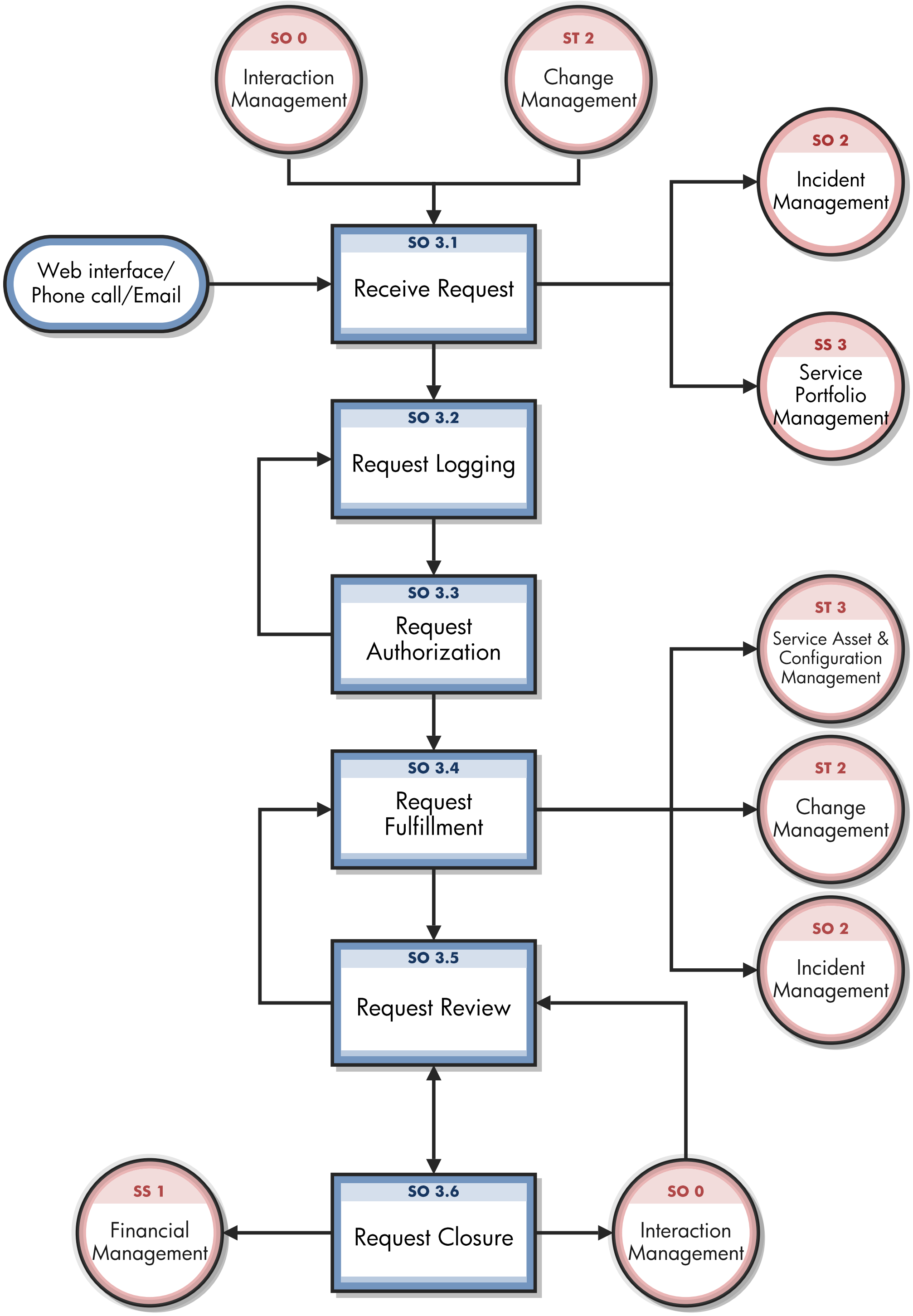
The authorization process automates and formalizes the technical and business evaluation by the appropriate levels of management of requests. Authorizations control accepts risk, cost, and responsibility of a request and its tasks. Authorizations create "chains" of groups who may be required to approve requests before they can advance within their lifecycle. Authorizations can have conditions attached, such as total cost, lead time requirements, and impact.

Authorizations can be defined either in request model or in the dedicated Authorization phase of the request fulfillment workflow.

Request Fulfillment process overview

The Request Fulfillment process includes the activities required to select items from service catalog and submit a service request, to give financial and business approvals, to provision, and to fulfill service requests. It is responsible for ensuring that an IT support is offered for self-help practices and requests can be effectively fulfilled after needed authorizations.

A general overview of the Request Fulfillment processes and workflows is depicted in the figure below. These workflows are described in detail in "Request Fulfillment Workflows" on page 304.


SO 0
Interaction Management
ST 2
Change Management
SO 2
Incident Management
Web interface/ Phone call/Email
SO 3.1
Receive Request
SS 3
Service Portfolio Management
SO 3.2
Request Logging
SO 3.3
Request Authorization
ST 3
Service Asset & Configuration Management
SO 3.4
Request Fulfillment
ST 2
Change Management
SO 2
Incident Management
SO 3.5
Request Review
SS 1
Financial Management
SO 3.6
Request Closure
SO 0
Interaction Management

Request Fulfillment user roles

The following table describes the responsibilities of Request Fulfillment user roles.

Request Fulfillment user roles

Role	Responsibilities
Request Process Owner	• Designs request fulfillment models and workflows. • Ensures process technicians have the required knowledge and the required technical and business understanding to deliver the process, and understand their role in the process. • Communicates process information or changes as appropriate to ensure awareness. • Reviews opportunities for process enhancements and for improving the efficiency and effectiveness of the process. • Works with other process owners to ensure there is an integrated approach to the design and implementation of request fulfillment, incident management, event management, access management, and problem management.
User	• Uses Self Service or the Service Desk to log appropriate Service Requests.
Requester	• Initiates a Service Request through the Request Fulfillment portal on behalf of users.
Request Coordinator	• Provides a single point of contact and end-to-end responsibility to ensure submitted Service Requests have been processed. • Provides initial triage of Service Requests to determine which IT resources should be engaged to fulfill them. • Assigns a Service Request to the correct group. • Communicates Service Requests to other IT resources that will be involved in fulfilling them. • Escalates Service Requests in line with established Service Level Targets.
Request Analyst	• Carries out one or more activities in the fulfillment of Service Requests. • Updates the records to show that activities have been carried out correctly. • Responsible for the provisioning of Service Requests within the agreed SLA.
Request Approver	• Reviews Service Request details. • Confirms Service Request details are correct. • Approves/Rejects Service Requests.
Request Manager	• Plans and manages support for request fulfillment tools and processes. • Handles staff, customer and management concerns, requests, issues and enquiries.

Request Fulfillment user roles, continued

Role	Responsibilities
	• Involved in Service Request escalation. • Ensures request fulfillment activities operate in line with service level targets.
Stock Manager	• Responsible for managing stock and defining reorder rules for different stockrooms.

Input and output for Request Fulfillment

Requests can be triggered and resolved in several ways. The following table outlines the inputs and outputs for the Request Fulfillment process.

Input and output for Request Fulfillment

Input to Request Fulfillment	Output from Request Fulfillment
• Service Requests • RFCs • Requests from various sources such as phone calls, web interfaces, or emails • Request for information	• Authorized/rejected service requests • Request fulfillment status reports • Fulfilled service requests • Incidents (rerouted) • RFCs/standard changes • Asset/CI updates • Updated request records • Closed service requests

Key performance indicators for Request Fulfillment

The Key Performance Indicators (KPIs) in the following table are useful for evaluating your Request Fulfillment 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 Request Fulfillment

Title	Description
Number of service requests	The total number of Service Requests. The indicator is used as a control measure.
Size of backlog	The size of current backlog of outstanding service.
Elapsed time	The mean elapsed time for handling each type of Service Requests.
Average cost	The average cost per type of Service Request.
Customer satisfaction	The level of user satisfaction with the handling of Service Requests (as measured in some form of satisfaction survey).

For completeness, the ITIL 2011 CSFs and KPIs are included below.

ITIL 2011 Critical Success Factors and Key Performance Indicators

The following are ITIL 2011 CSFs and KPIs for Request Fulfillment:

- **CSF** - Requests must be fulfilled in an efficient and timely manner that is aligned to agreed service level targets for each type of request
    - **KPI** - The mean elapsed time for handling each type of service request
    - **KPI** - The number and percentage of service requests completed within agreed target times
    - **KPI** - Breakdown of service requests at each stage (e.g. logged, work in progress, closed etc.)
    - **KPI** - Percentage of service requests closed by the service desk without reference to other levels of support (often referred to as "first point of contact")
    - **KPI** - Number and percentage of service requests resolved remotely or through automation, without the need for a visit
    - **KPI** - Total numbers of requests (as a control measure)
    - **KPI** - The average cost per type of service request
- **CSF** - Only authorized requests should be fulfilled

- ○ **KPI** - Percentage of service requests fulfilled that were appropriately authorized
- ○ **KPI** - Number of incidents related to security threats from request fulfillment activities

- **CSF** - User satisfaction must be maintained
  - **KPI** - Level of user satisfaction with the handling of service requests (as measured in some form of satisfaction survey)
  - **KPI** - Total number of incidents related to request fulfillment activities
  - **KPI** - The size of current backlog of outstanding service requests.

RACI matrix for Request Fulfillment

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 Request Fulfillment is shown in the following table.

RACI matrix for Request Fulfillmen

Process ID	Activity	User/Requester	Request Coordinator	Request Analyst	Request Approver	Request Manager
SO 3.1	Receive Request	R	R			A
SO 3.2	Request Logging		R			A
SO 3.3	Request Authorization	I	C		R	A
SO 3.4	Request Fulfillment	I	R	R		A/C
SO 3.5	Request Review		C			A/R
SO 3.6	Request Closure	I	R			A

Chapter 20: Request Fulfillment Workflows

The Request Fulfillment process includes the activities required to select items from service catalog and submit a service request, to give financial and business approvals, to provision, and to fulfill service requests. It is responsible for ensuring that an IT support is offered for self-help practices and requests can be effectively fulfilled after needed authorizations.

The Request Fulfillment process consists of the following processes, which are included in this chapter:

- "Receive Request (process SO 3.1)" on the next page
- "Request Logging (process SO 3.2)" on page 308
- "Request Authorization (process SO 3.3)" on page 309
- "Request Fulfillment (process SO 3.4)" on page 310
- "Request Review (process SO 3.5)" on page 314
- "Request Closure (process SO 3.6)" on page 315

Receive Request (process SO 3.1)

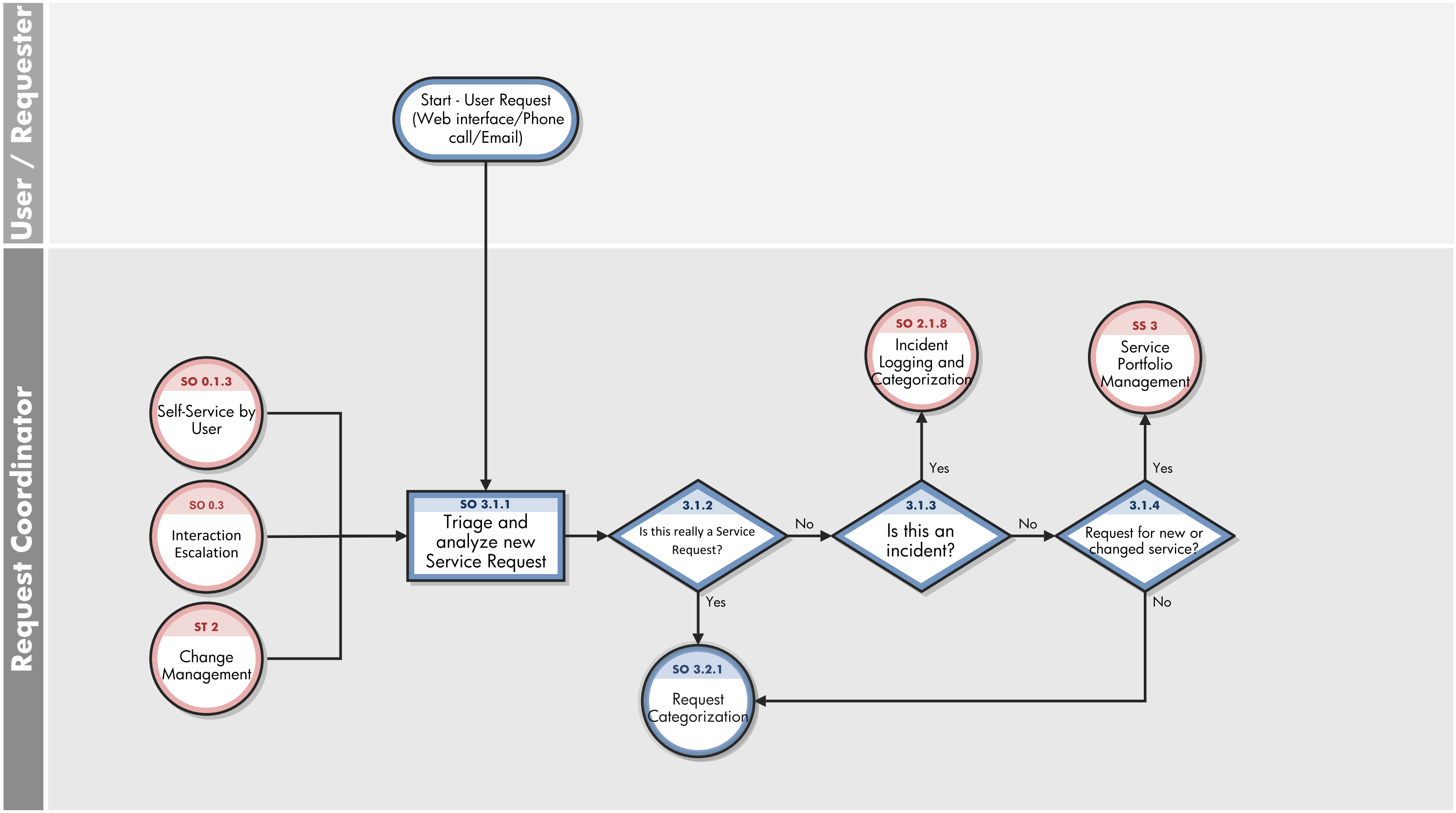
Fulfillment work on service requests should not begin until a formalized request is received.The Receive Request process starts when a User or Requester uses Self Service or the Service Desk to log appropriate Service Requests. It is also usual to have requests that come in from other sources such as RFCs, emails, web interfaces, or phone calls. A Service Request submitted by the User or Requester can be a request for existing Service Catalog, a request for a new service, or an amendment to the Service Catalog. The Request Coordinator needs to triage and analyze the request, and then decide what to do next. As a result of the Receive Request process, a Service Request will be logged.

The following user roles can perform Receive Request:

- User or Requester
- Request Coordinator

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

The Receive Request workflow is illustrated in the following figure:


User / Requester
Request Coordinator
Start - User Request (Web interface/Phone call/Email)
SO 0.1.3
Self-Service by User
SO 0.3
Interaction Escalation
ST 2
Change Management
SO 3.1.1
Triage and analyze new Service Request
3.1.2
Is this really a Service Request?
Yes
No
SO 3.2.1
Request Categorization
3.1.3
Is this an incident?
Yes
No
SO 2.1.8
Incident Logging and Categorization
3.1.4
Request for new or changed service?
Yes
No
SS 3
Service Portfolio Management

Receive Request process

Process ID	Procedure or Decision	Description	Role
SO 3.1.1	Triage and analyze the new Service Request	New Service Requests mostly come from the Service Desk or Service Catalog. It is also usual to have requests that come in from RFCs, emails, web interfaces or phone calls. Based on the information provided by User or Requester, Request Coordinator will triage and analyze the new Service Request from different sources.	Request Coordinator
SO 3.1.2	Is this really a Service Request?	Initially, it must be determined whether the request is really a Service Request or not. If yes, go to SO 3.2.1 to log the Service Request. If no, go to SO 3.1.3.	Request Coordinator
SO 3.1.3	Is this an Incident?	In some cases, an Incident has taken place, but a Service Request is reported. If this is the case, go to SO 2.1.8 to create a new Incident. The Service Request and any related information should be forwarded to Incident Management. If not, go to SO 3.1.4.	Request Coordinator
SO 3.1.4	Request for new or changed service?	In other cases, the request may actually be a request for new or changed service features. If this is the case, the Service Request will be passed to the Service Portfolio Management processes to properly review the need and business case for the service change. If not, go to SO 3.2.1 to log the Service Request.	Request Coordinator

Request Logging (process SO 3.2)

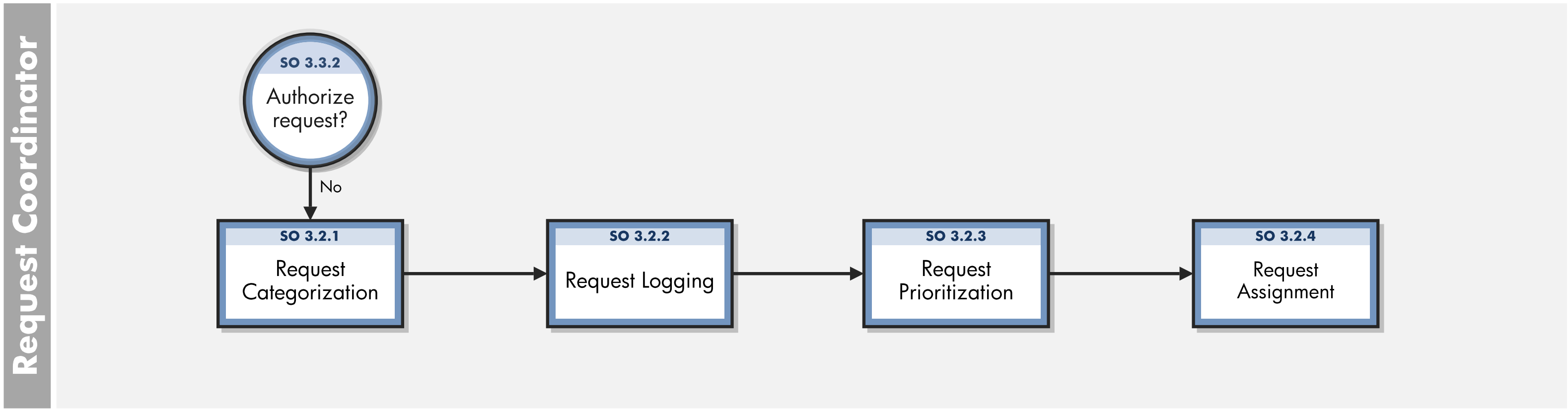
All Service Requests must be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk, RFC, telephone call, or email. Allocating suitable request categorization code should take place at the very beginning of the logging process, so that the exact type of the request is recorded. Besides the categorization code, allocating appropriate prioritization code and determining assignment group/person to fulfill the request are also the important steps in the Request Logging process.

The following user roles can perform Request Logging:

- Request Coordinator

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

The Request Logging workflow is illustrated in the following figure:



Request Logging process

Process ID	Procedure or Decision	Description	Role
SO 3.2.1	Request Categorization	Before request details are recorded, the appropriate request model (grouped by request category/sub-category) or request category should be chosen based on the type of request being fulfilled.	Request Coordinator
SO 3.2.2	Request Logging	All relevant information of the request must be logged so that a full historical record is maintained. The information needed for a Service Request is listed in the "Request Fulfillment Details" section.	Request Coordinator
SO 3.2.3	Request Prioritization	Appropriate prioritization code helps to determine how the Service Request is handled by support tools and support staff. Prioritization can normally be determined by both the urgency of the request (how quickly the business needs to have it fulfilled) and the level of impact it is causing.	Request Coordinator
SO 3.2.4	Request Assignment	In the request logging stage, the assignment group/person of the Service Request is determined either by a pre-defined assignment rule or Request Coordinator.	Request Coordinator

Request Authorization (process SO 3.3)

No work should take place to fulfill a request until it has been properly authorized. Simple requests can be pre-authorized, while a more rigorous authorization may be needed for other requests before any work can proceed.

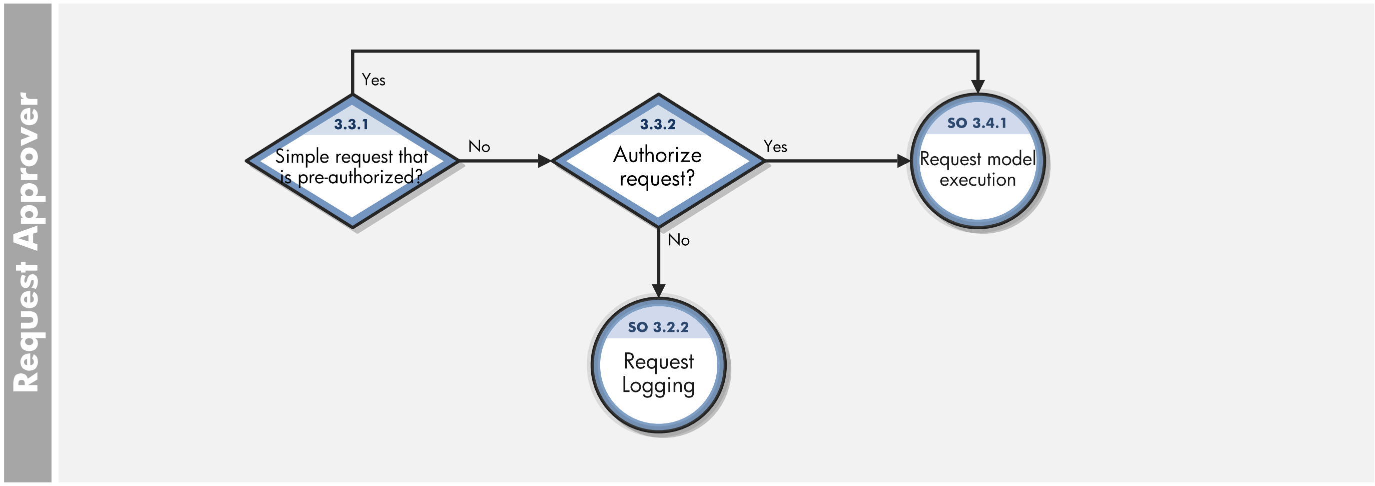
A Service Request that cannot be properly authorized should be returned to the Request Logging phase.

The following user roles can perform Request Authorization:

- Request Approver

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

The Request Authorization workflow is illustrated in the following figure:



Request Authorization process

Process ID	Procedure or Decision	Description	Role
SO 3.3.1	Simple request that is pre-authorized?	If it is a simple request that does not require a dedicated authorization, go to SO 3.4.1 to execute the request model. If a more rigorous authorization is required, go to SO 3.3.2 for request authorization.	Request Approver
SO 3.3.2	Authorize request?	Request Approver reviews the Service Request details and decide to approve or deny the request. If request is approved, go to SO 3.4.1 to execute the request model. If request is denied, go to SO 3.3.3.	Request Approver

Request Fulfillment (process SO 3.4)

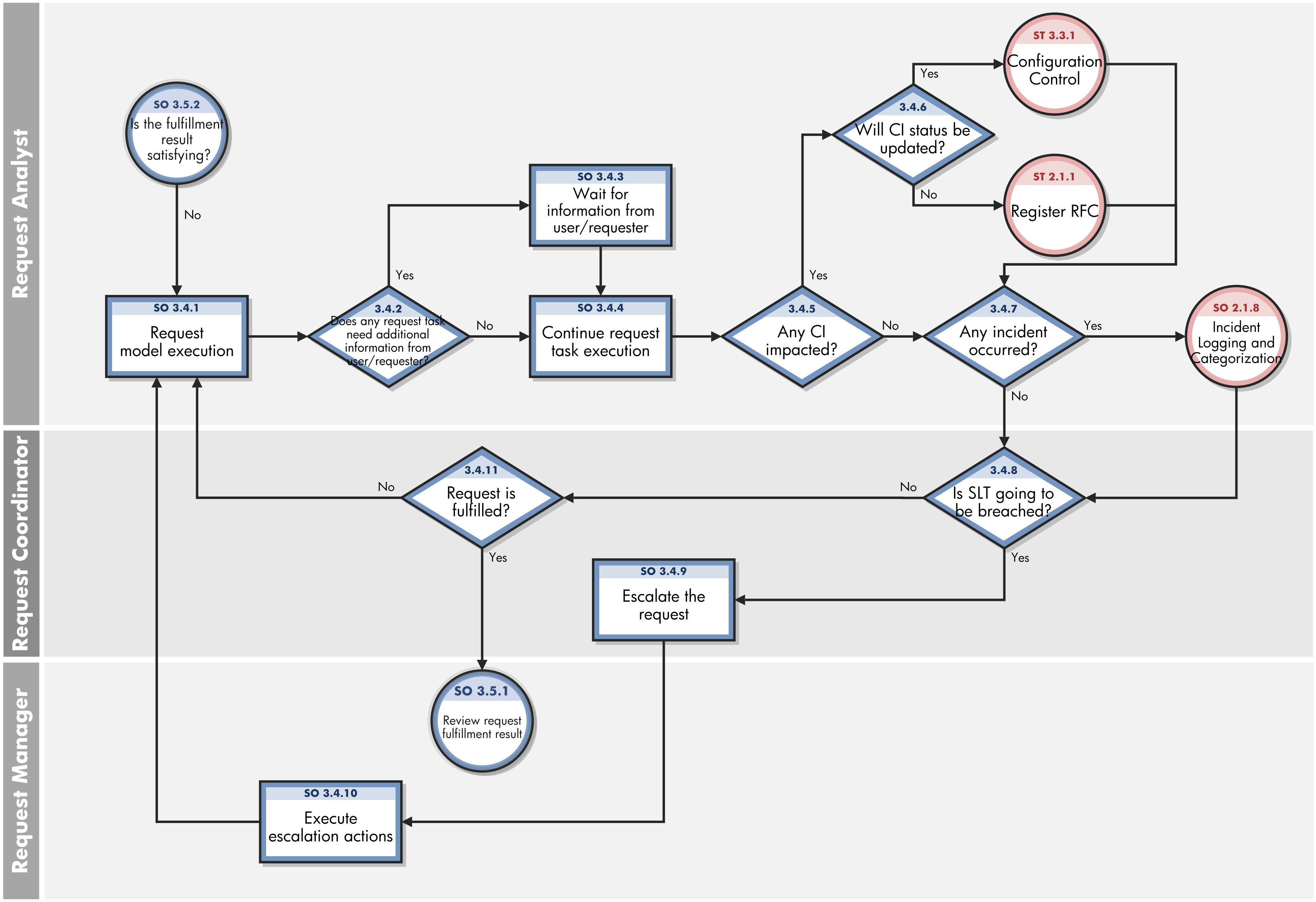
In the Request Fulfillment process, the process steps and activities indicated in the request model are executed by the assignment group/person to fulfill the request. The process steps and activities are created as request tasks.

The following user roles can perform Request Fulfillment:

- Request Coordinator
- Request Analyst
- Request Manager

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

The Request Fulfillment workflow is illustrated in the following figure:


Request Analyst
Request Coordinator
Request Manager
SO 3.5.2
Is the fulfillment result satisfying?
No
SO 3.4.1
Request model execution
3.4.2
Does any request task need additional information from user/requester?
Yes
No
SO 3.4.3
Wait for information from user/requester
SO 3.4.4
Continue request task execution
3.4.5
Any CI impacted?
Yes
No
3.4.6
Will CI status be updated?
Yes
No
ST 3.3.1
Configuration Control
ST 2.1.1
Register RFC
3.4.7
Any incident occurred?
Yes
No
SO 2.1.8
Incident Logging and Categorization
3.4.8
Is SLT going to be breached?
No
Yes
3.4.11
Request is fulfilled?
No
Yes
SO 3.4.9
Escalate the request
SO 3.5.1
Review request fulfillment result
SO 3.4.10
Execute escalation actions

Request Fulfillment process

Process ID	Procedure or Decision	Description	Role
SO 3.4.1	Request Model Execution	The request tasks defined in the request model are executed by the Request Analyst who is the task assignee. In some cases, additional tasks out of the request model may be added and executed in a request record if necessary.	Request Analyst
SO 3.4.2	Does any request task need additional information from user/requester?	During request fulfillment, Request Analyst checks whether the information provided to fulfill the request is enough or not. If yes, go to SO 3.4.3. If no, go to SO 3.4.4.	Request Analyst
SO 3.4.3	Waiting for information provided from user/requester	Request task status is set as “Pending Customer” and a “Visible to Customer” update is added, so that User or Requester will be informed.	Request Analyst
SO 3.4.4	Continue request task execution	Request Analyst continues task execution with sufficient information provided by User or Requester.	Request Analyst
SO 3.4.5	Any CI impacted?	Request Analyst checks whether CIs are impacted during request fulfillment process. If yes, go to SO 3.4.6. If no, go to SO 3.4.7.	Request Analyst
SO 3.4.6	Will CI status be updated?	If only CI status needs to be updated or new CIs are going to be created, go to the Service Asset & Configuration Management process (ST 3.3.1) to review and update the CIs. If no, go to the Change Management process (ST 2.1.1) to raise and log RFC.	Request Analyst
SO 3.4.7	Any incident occurred?	If an incident occurs during request fulfillment process, the new incident will be created by the Incident Management process (SO 2.1.8) and related to the request. If no incident occurs, go to SO 3.4.8.	Request Analyst
SO 3.4.8	Is SLT going to be breached?	In the whole request fulfillment process, Request Coordinator keeps monitoring the Service Level Target. If SLT is going to be breached, Request Coordinator will escalate the request in time (SO 3.4.9). If no, go to SO 3.4.11.	Request Coordinator
SO 3.4.9	Escalate the request	Request Coordinator indicates the responsible Request Manager whom the Service Request will be escalated to.	Request Coordinator

Request Fulfillment process, continued

Process ID	Procedure or Decision	Description	Role
SO 3.4.10	Execute escalation actions	The Request Manager determines the actions to be performed to fulfill the request within the target time and designates the persons to execute the actions.	Request Manager
SO 3.4.11	Request is fulfilled?	Request Coordinator looks up the execution progress of request tasks and if all tasks are finished, go to SO 3.5.1 to review the fulfillment result. If some tasks are not closed, go to SO 3.4.1 to continue task execution in request model.	Request Coordinator

Request Review (process SO 3.5)

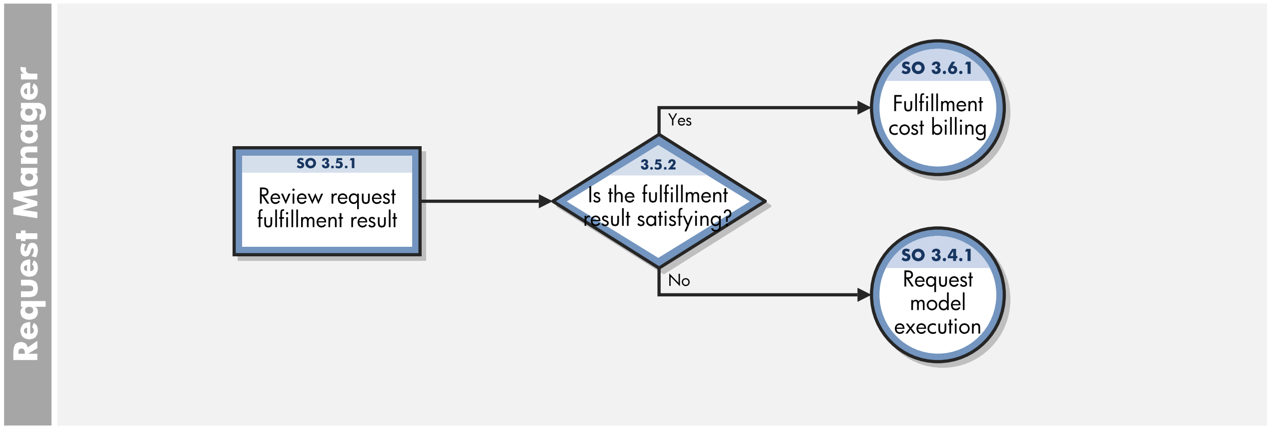
After a request is fulfilled, the accountable person should review the fulfillment result including the fulfillment costs, whether the fulfillment activities are in line with Service Level Target, and so on.

The following user role can perform Request Review:

- Request Manager

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

The Request Review workflow is illustrated in the following figure:



Request Review process

Process ID	Procedure or Decision	Description	Role
SO 3.5.1	Review request fulfillment result	The Request Manager reviews the request fulfillment result, including the costs for the fulfillment activities, whether Service Level Target has been achieved, and so on.	Request Manager
SO 3.5.2	Is the fulfillment result satisfying?	Request Manager decides whether the fulfillment result is satisfying. If yes, go to SO 3.6.1. If no, go to SO 3.4.1 to re-fulfill the request.	Request Manager

Request Closure (process SO 3.6)

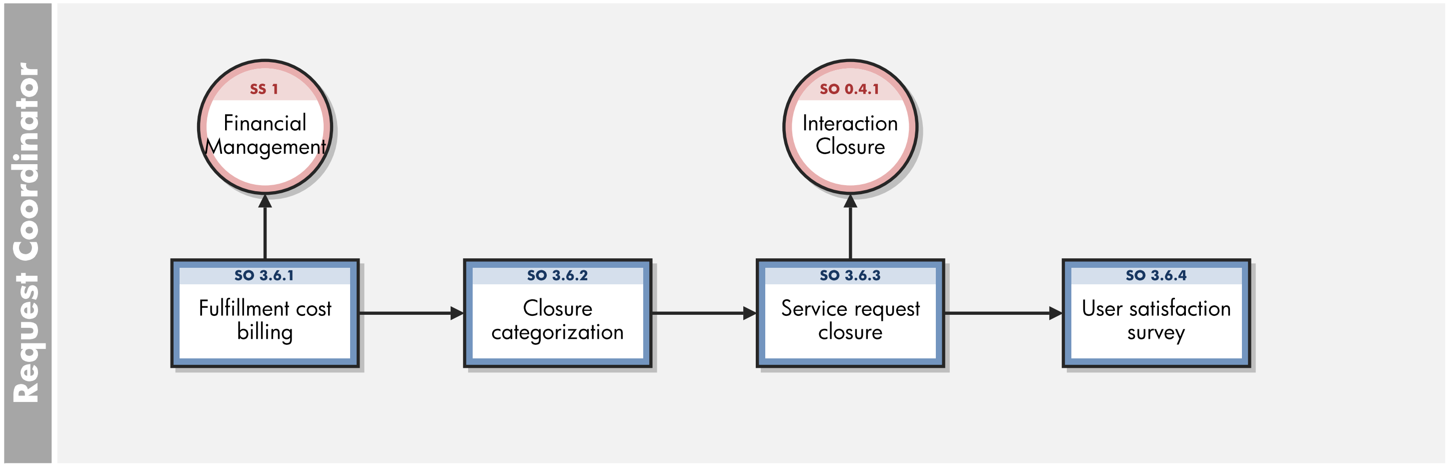
Once the Service Request activities are completed, the Financial Management process might be involved for fulfillment cost billing. When the closure action happens, request categorization should be checked and confirmed. When a request is closed, Service Desk will be notified of the completion status, and the Service Desk will communicate with User or Requester on the fulfillment result. User satisfaction survey can also be carried out for some requests.

The following user role can perform Request Closure:

- Request Coordinator

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

The Request Closure workflow is illustrated in the following figure:



Request Closure process

Process ID	Procedure or Decision	Description	Role
SO 3.6.1	Fulfillment cost billing	The Financial Management process will need to be notified of any costs incurred by the fulfillment activities.	Request Coordinator
SO 3.6.2	Closure categorization	When the closure action happens, request categorization will be checked and confirmed. If the categorization subsequently turns out to be incorrect, Request Coordinator will update the request record so that a correct closure categorization is recorded for the request. Request Coordinator can ask for advice or guidance from the fulfillment groups as necessary.	Request Coordinator
SO 3.6.3	Service request	When the Service Request is formally closed, Service Desk will be notified of the completion status and the related Interaction will be updated accordingly (SO 0.4.1). Service Desk then communicates with	Request Coordinator

Request Closure process, continued

Process ID	Procedure or Decision	Description	Role
	closure	User or Requester on the fulfillment result. In case User or Requester is unsatisfied with the fulfillment result, the request record may be re-opened.	
SO 3.6.4	User satisfaction survey	A user satisfaction survey can be carried out for the agreed percentage of closed requests.	Request Coordinator

Chapter 21: Request Fulfillment Details

HP Service Manager uses the Request Fulfillment application to enable the Request Fulfillment process. The main function of Request Fulfillment is to standardize the methods and processes a business organization uses to log, approve, validate, monitor, and escalate service requests as necessary.

This section describes selected Request Fulfillment fields in the out-of-box Service Manager system.

Topics in this section include:

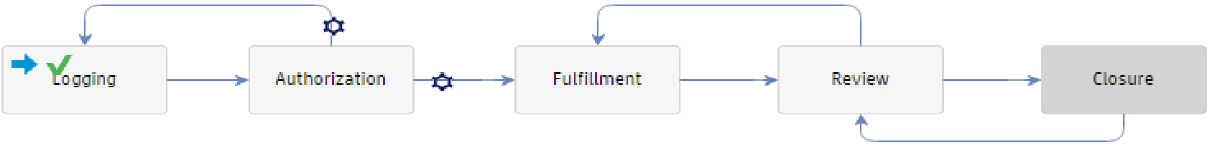
- "Request Fulfillment process flow" below
- "Request Fulfillment forms" on page 320
- "Request Fulfillment form details" on page 324
- "Request task forms" on page 331
- "Request task form details" on page 335

Request Fulfillment process flow

The Request Fulfillment process flow in Service Manager is as follows.

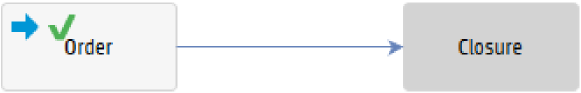
Generic Request workflow

This workflow addresses the request fulfillment process. Its associated request category is “Generic Request.”



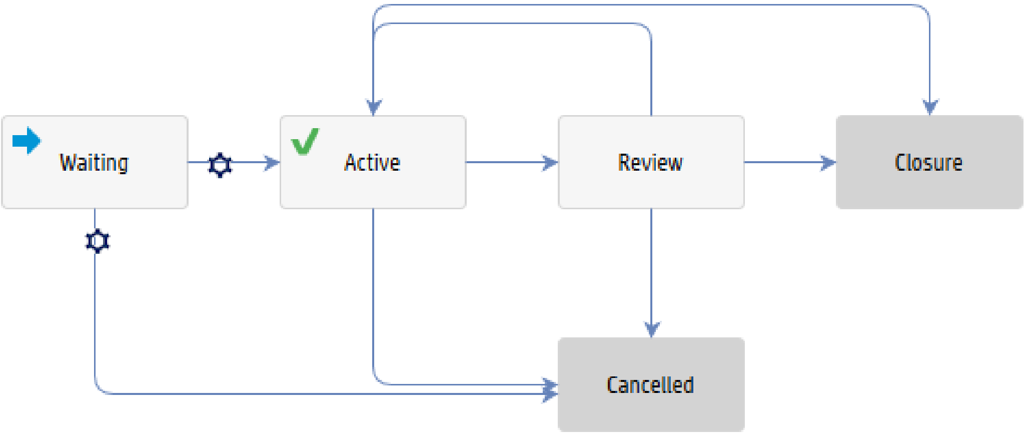
Order workflow

The order workflow is used for purchase and stock management in Request Fulfillment application. Its associated request category is “Order.”

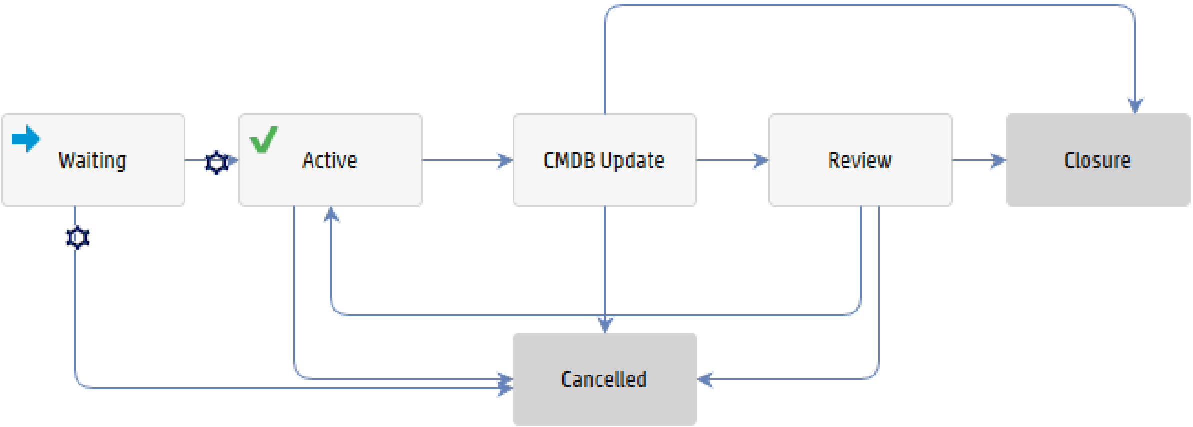


Request task workflows

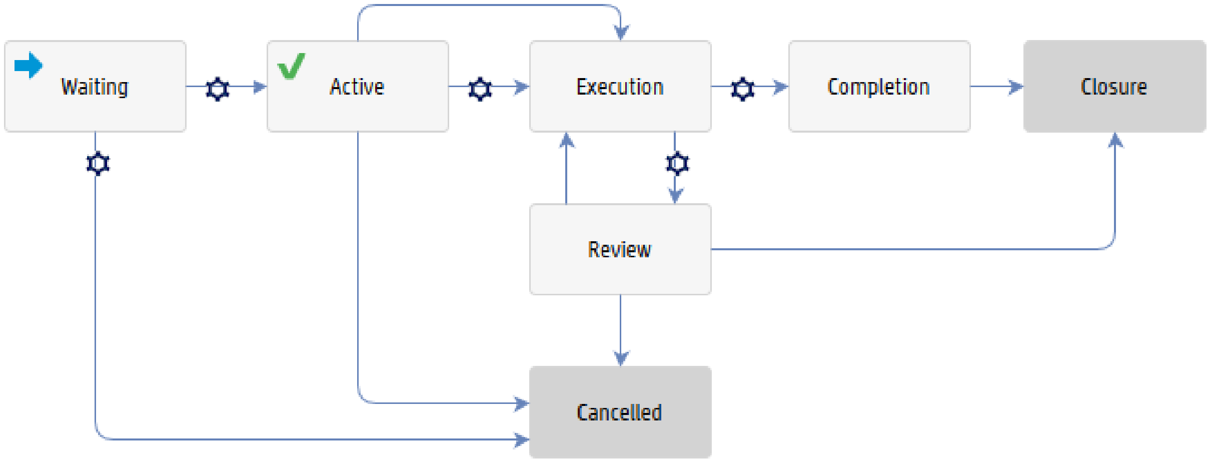
The following is the request task workflow without CMDB update. Its associated request task category is “Labor.”



The following is the request task workflow with CMDB update. Its associated request task categories are “Purchase,” “Reservation,” “Installation,” and “Uninstallation.”



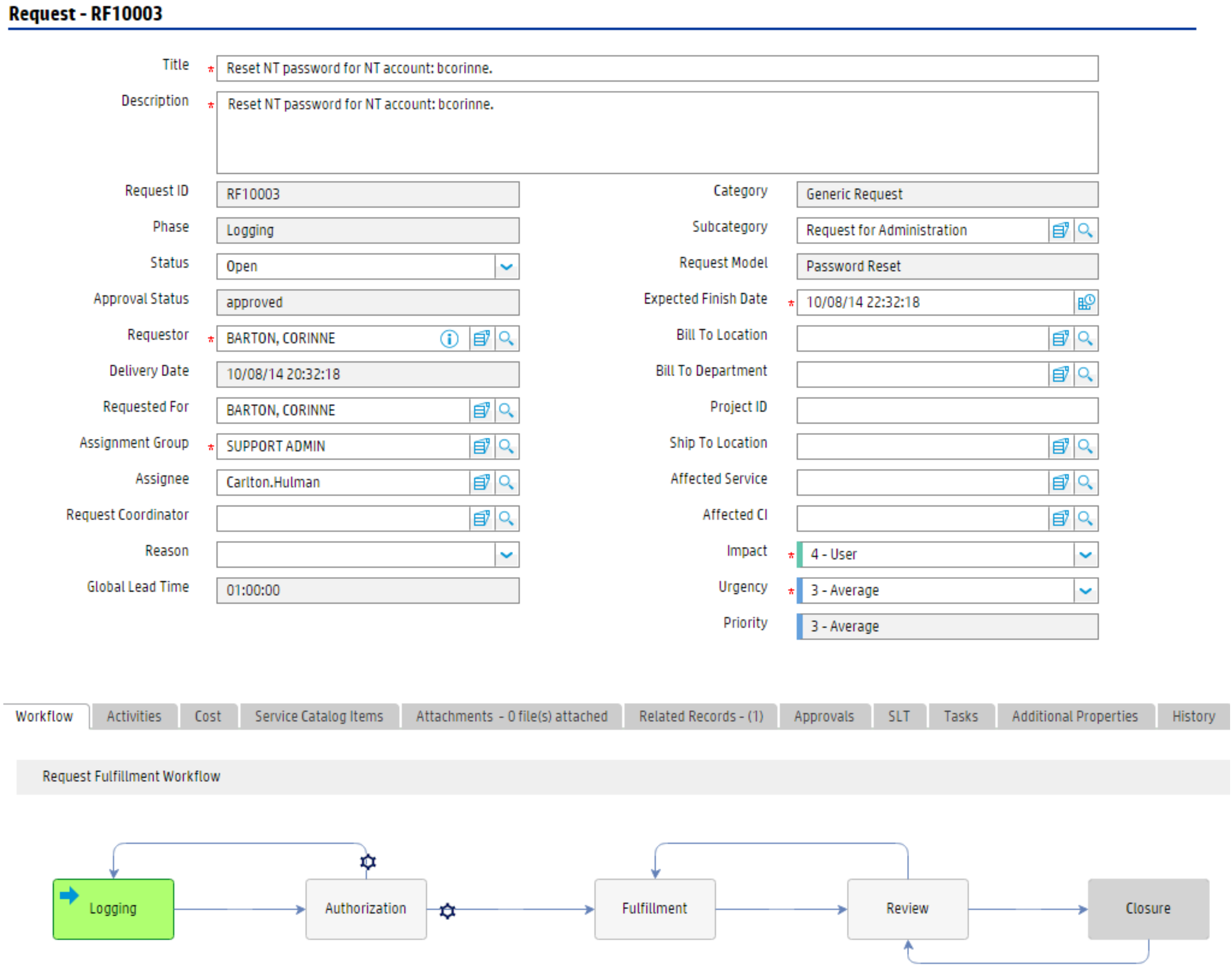
The following is the request task workflow for automation (OO flow execution). Its associated request task category is “Automation.”



Request Fulfillment forms

Generic Request forms

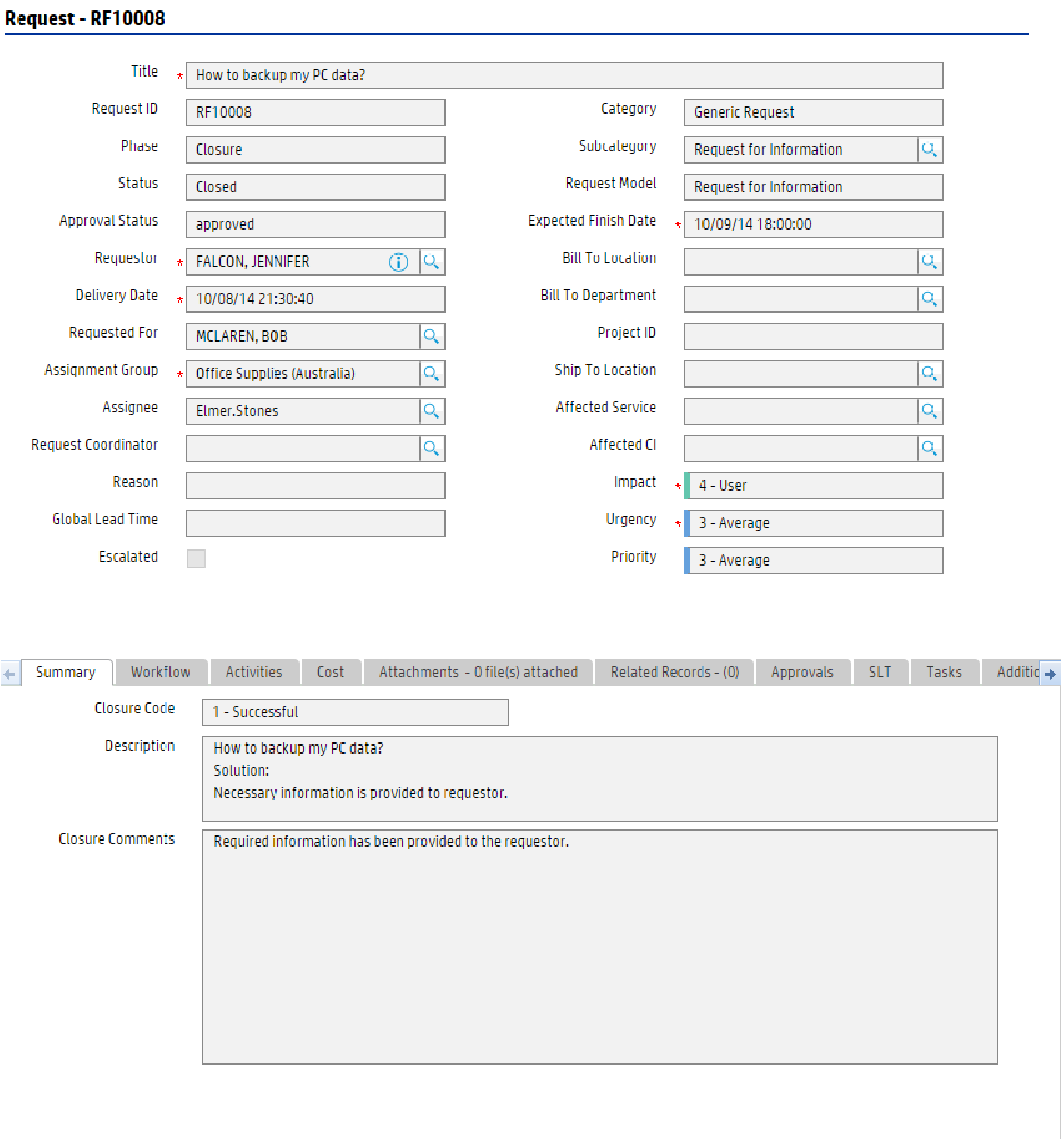
The following figure shows the open request form that associated with the generic request workflow.



Request - RF10003

Title *	Reset NT password for NT account: bcorinne.		
Description *	Reset NT password for NT account: bcorinne.		
Request ID	RF10003	Category	Generic Request
Phase	Logging	Subcategory	Request for Administration
Status	Open	Request Model	Password Reset
Approval Status	approved	Expected Finish Date *	10/08/14 22:32:18
Requestor *	BARTON, CORINNE	Bill To Location	
Delivery Date	10/08/14 20:32:18	Bill To Department	
Requested For	BARTON, CORINNE	Project ID	
Assignment Group *	SUPPORT ADMIN	Ship To Location	
Assignee	Carlton.Hulman	Affected Service	
Request Coordinator		Affected CI	
Reason		Impact *	4 - User
Global Lead Time	01:00:00	Urgency *	3 - Average
		Priority	3 - Average

The following figure shows the closed request form that associated with the generic request workflow.



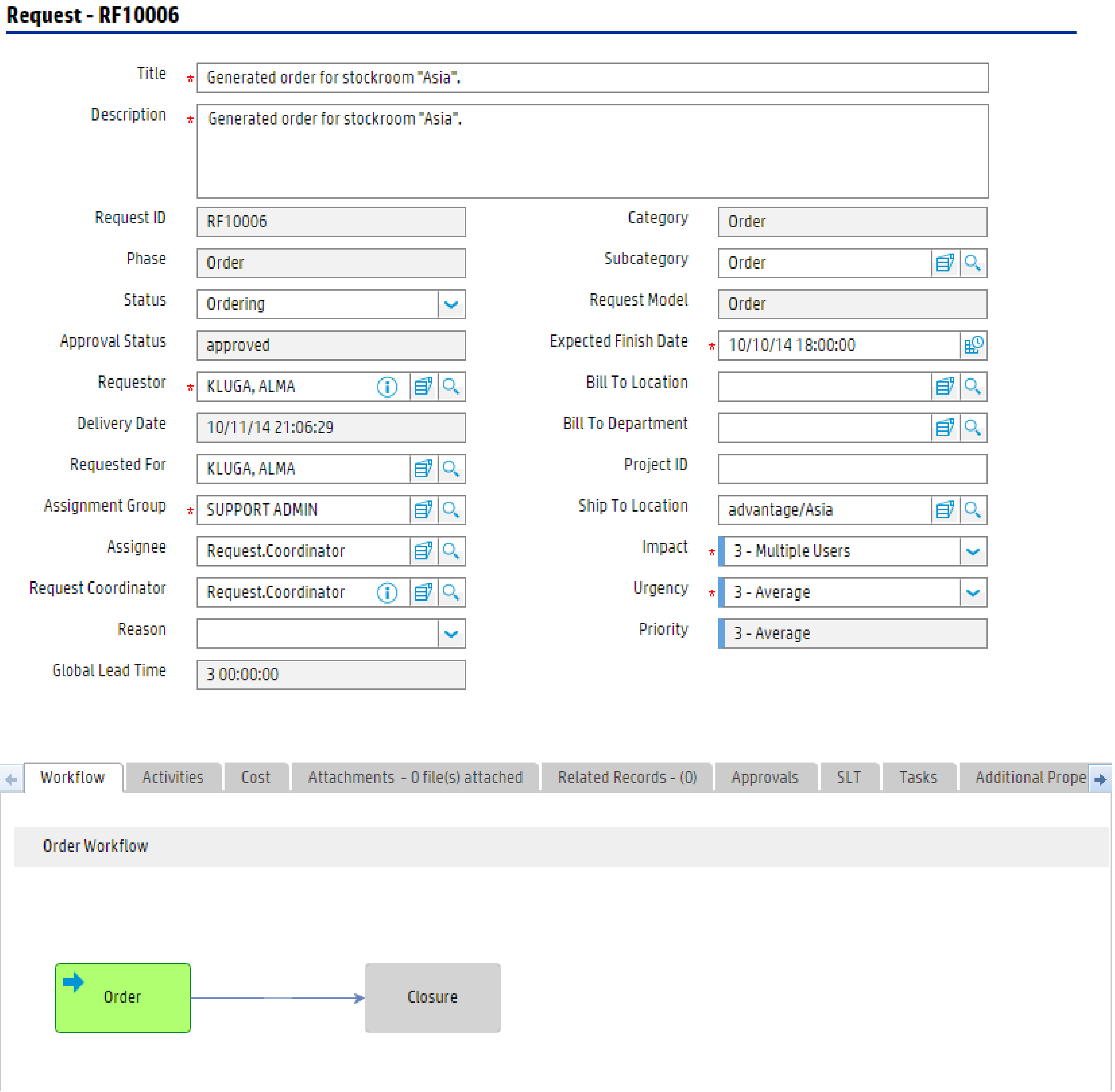
Request - RF10008

Title *	How to backup my PC data?		
Request ID	RF10008	Category	Generic Request
Phase	Closure	Subcategory	Request for Information
Status	Closed	Request Model	Request for Information
Approval Status	approved	Expected Finish Date *	10/09/14 18:00:00
Requestor *	FALCON, JENNIFER	Bill To Location	
Delivery Date *	10/08/14 21:30:40	Bill To Department	
Requested For	MCLAREN, BOB	Project ID	
Assignment Group *	Office Supplies (Australia)	Ship To Location	
Assignee	Elmer.Stones	Affected Service	
Request Coordinator		Affected CI	
Reason		Impact *	4 - User
Global Lead Time		Urgency *	3 - Average
Escalated	□	Priority	3 - Average

Closure Code	1 - Successful
Description	How to backup my PC data? Solution: Necessary information is provided to requestor.
Closure Comments	Required information has been provided to the requestor.

Order forms

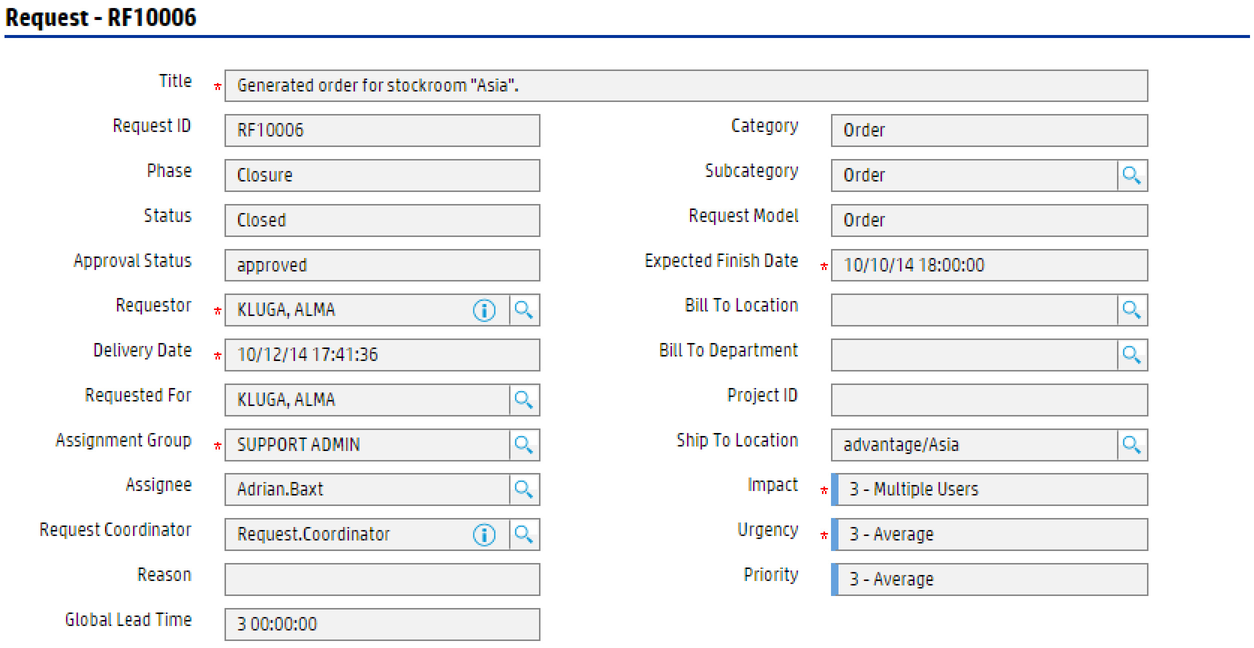
The following figure shows the open order form that associated with the order workflow.



Request - RF10006

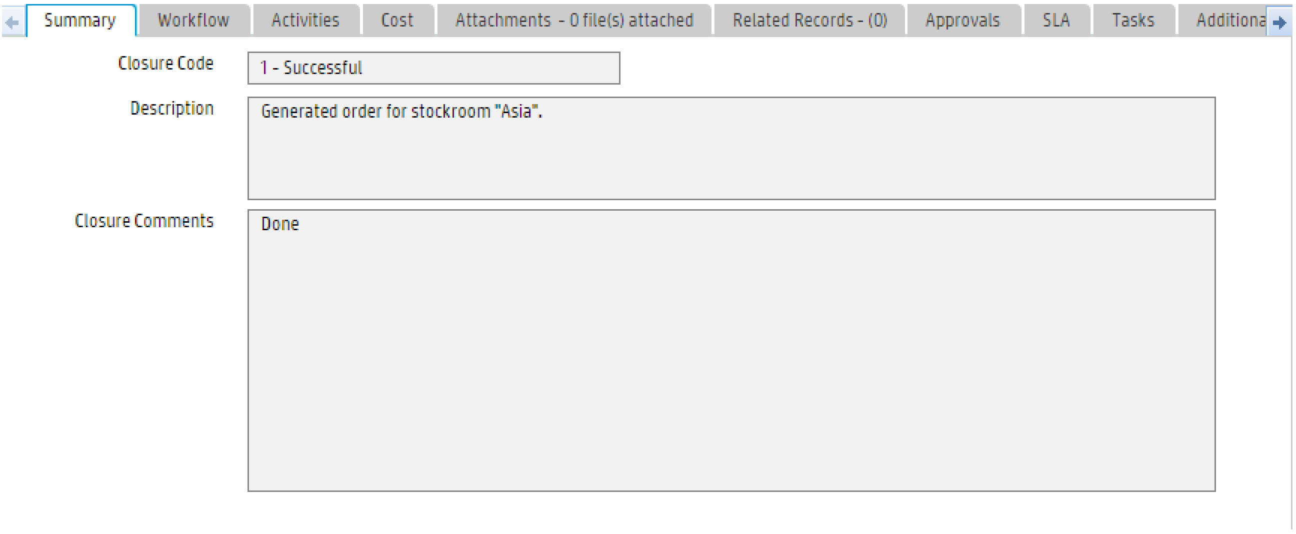
Title	* Generated order for stockroom "Asia".		
Description	* Generated order for stockroom "Asia".		
Request ID	RF10006	Category	Order
Phase	Order	Subcategory	Order
Status	Ordering	Request Model	Order
Approval Status	approved	Expected Finish Date	* 10/10/14 18:00:00
Requestor	* KLUGA, ALMA	Bill To Location	
Delivery Date	10/11/14 21:06:29	Bill To Department	
Requested For	KLUGA, ALMA	Project ID	
Assignment Group	* SUPPORT ADMIN	Ship To Location	advantage/Asia
Assignee	Request.Coordinator	Impact	* 3 - Multiple Users
Request Coordinator	Request.Coordinator	Urgency	* 3 - Average
Reason		Priority	3 - Average
Global Lead Time	3 00:00:00		

The following figure shows the closed order form that associated with the order workflow.



Request - RF10006

Title *	Generated order for stockroom "Asia".		
Request ID	RF10006	Category	Order
Phase	Closure	Subcategory	Order
Status	Closed	Request Model	Order
Approval Status	approved	Expected Finish Date *	10/10/14 18:00:00
Requestor *	KLUGA, ALMA	Bill To Location	
Delivery Date *	10/12/14 17:41:36	Bill To Department	
Requested For	KLUGA, ALMA	Project ID	
Assignment Group *	SUPPORT ADMIN	Ship To Location	advantage/Asia
Assignee	Adrian.Baxt	Impact *	3 - Multiple Users
Request Coordinator	Request.Coordinator	Urgency *	3 - Average
Reason		Priority	3 - Average
Global Lead Time	3 00:00:00		



Closure Code	1 - Successful
Description	Generated order for stockroom "Asia".
Closure Comments	Done

Request Fulfillment form details

The following table identifies and describes some of the features on the Request Fulfillment form.

Request/Order field descriptions

Label	Description
Request ID	The system-generated unique ID for this request/order.
Title	A short description that summarizes the request/order. It is a mandatory field.
Description	A detailed description of the request/order. It is a mandatory field.
Category	This field describes the type of Service Request. In out-of-box, the following categories are available: • Generic Request • Order
Subcategory	Specifies the second level of classifying a Service Request. In out-of-box, the following subcategories are available for the “Generic Request” category : • Employee Off-boarding • Employee On-boarding • Hardware • Others • Request for Administration • Request for Access • Request for Information • Software In out-of-box, the following subcategory is available for the “Order” category: • Order
Request Model	A Request Model is a record that is used to predefine the contents of a specific type of Service Request, including the information used to populate the request/order and the tasks that are needed to complete the request/order. When you open a request/order using a Request Model, basic information is added to the request/order automatically.
Phase	This is a system-generated field that specifies the name of the current phase of the request/order. The following phases are available in out-of-box “Generic Request” workflow:

Request/Order field descriptions, continued

Label	Description
	• Logging • Authorization • Fulfillment • Review • Closure The following phases are available in out-of-box "Order" workflow: • Order • Closure
Status	Displays the status of the request/order. The following statuses are available in out-of-box “Generic Request” workflow: • Open - Request is logged and waiting for authorization. • In Progress - Request is being fulfilled. • Pending Customer - Additional information is required from user/requester. • Suspended - Fulfillment activities for the request have been suspended for a pre-defined time period. • Fulfilled - Request is fulfilled and being reviewed. • Closed - Request is closed. The following statuses are available in out-of-box "Order" workflow: • Ordering - Order is being handled. • Closed - Order is closed.
Approval Status	Defines the approval status for the request/order. The system sets this field depending on current approvals and the approval type defined for the record. These approval statuses are available out-of-box: • pending • approved • denied

Request/Order field descriptions, continued

Label	Description
Requester	The name of the person who submits the Service Request. It is a mandatory field.
Requested For	The name of the user for whom the requester submits this request/order.
Delivery Date	Indicates the target fulfillment time of request. It equals request creation time plus “Global Lead Time.”
Expected Finish Date	Indicates the expected finish date of request from user/requester perspective. If Delivery Target is selected when ordering is made from Service Catalog, the field value will be calculated by request creation time plus Delivery Target. If Delivery Target is not available for the request, the field value will leave blank when request is logged. In this case, Request Coordinator will manually input the expected date on behalf of user/requester. It is a mandatory field.
Assignment Group	The support group assigned to work on this request/order. This field can be prepopulated by the data defined in assignment rule or manually set by Request Coordinator. It is a mandatory field.
Assignee	The person assigned to work on this request/order. This person is a member of the assignment group. This field can be prepopulated by the data defined in assignment rule or manually set by Request Coordinator.
Request Coordinator	The name of the person responsible for coordinating the implementation of the request/order. Each Coordinator may belong to several assignment groups. Each group can have just one Request Coordinator.
Global Lead Time	This field is the sum of the longest “Planned Lead Time” of all request tasks based on task plan definition in Request Model. It is read-only and copied from Request Model. The out-of-box request fulfillment SLT is measured based on the value of this field.
Impact	A measure of the effect of the request/order on business processes. Impact and urgency are used to assign priority. It is a mandatory field. These impacts are available out-of-box: • Enterprise • Site/Dept • Multiple Users • User
Urgency	A measure of how long it will be until a request/order has a significant impact on the business. Impact and urgency are used to assign priority. It is a mandatory field.

Request/Order field descriptions, continued

Label	Description
	These urgencies are available out-of-box: • Critical • High • Average • Low
Priority	The order in which to address the request/order in comparison to others. The priority value is calculated using impact and urgency.
Reason	Select the reason for requesting the request/order: • Conversion • Customer Request • Legal • Maintenance • New • Problem Resolution
Ship To Location	The destination location the requested items should be shipped to.
Affected Service	Specifies the service that is affected by the request/order.
Affected CI	Specifies the CI that is affected by the request/order. Affected CI is one of the children of affected service.
Bill To Location	The location where the invoice should be mailed for the items shipped. Available locations are defined in System Administration > Base System Configuration > Locations.
Bill To Department	The department where the invoice should be sent for the items shipped. The departments available for selection are defined in **System Administration** > **Base System Configuration** > **Departments**.
Project ID	The identification number given to the project.
Escalated	If selected (set to true), this field indicates that the request needs to be escalated to Request Manager.
Request Manager	This field is only visible when “Escalated” is selected. It indicates the person who will handle the request escalation.
Cost > Total Cost	Total cost incurred by fulfillment activities, including cost of part items and

Request/Order field descriptions, continued

Label	Description
	labor cost.
Cost > Currency	Specifies the currency of the total cost.
Cost > Date/Technician/Hours Worked	The table specifies when and who will work on the request/order for how many hours. The labor cost is calculated based on the hourly rate of the technician and the hours that he/she worked.
Summary > Closure Code	Specifies a predefined closure code to describe how the request/order has been fulfilled. These closure codes are available out-of-box: • Successful • Successful (with problems) • Failed • Rejected (financial) • Rejected (technical) • Rejected (security) • Withdrawn • Withdrawal requested by customer • Cancelled • Denied request fulfillment
Summary > Closure Comments	This field is to document additional comments to close the request/order.
Workflow section	Displays a figure of generic request workflow/order workflow. It indicates the current phase which the request/order is in, and traces the phase transition history.
Activities section	Records information that the operator enters during the lifecycle of the request/order. Every time you update a request/order, you can fill in an update on the Activities section (New Update) with or without “Visible to Customer” flagged. A log of all the updates is stored on the Journal Updates and activities list. Updates from user/requester also display here with activity type “Update from customer.”
Attachments section	You can use the Attachments section to attach documents to request/order.

Request/Order field descriptions, continued

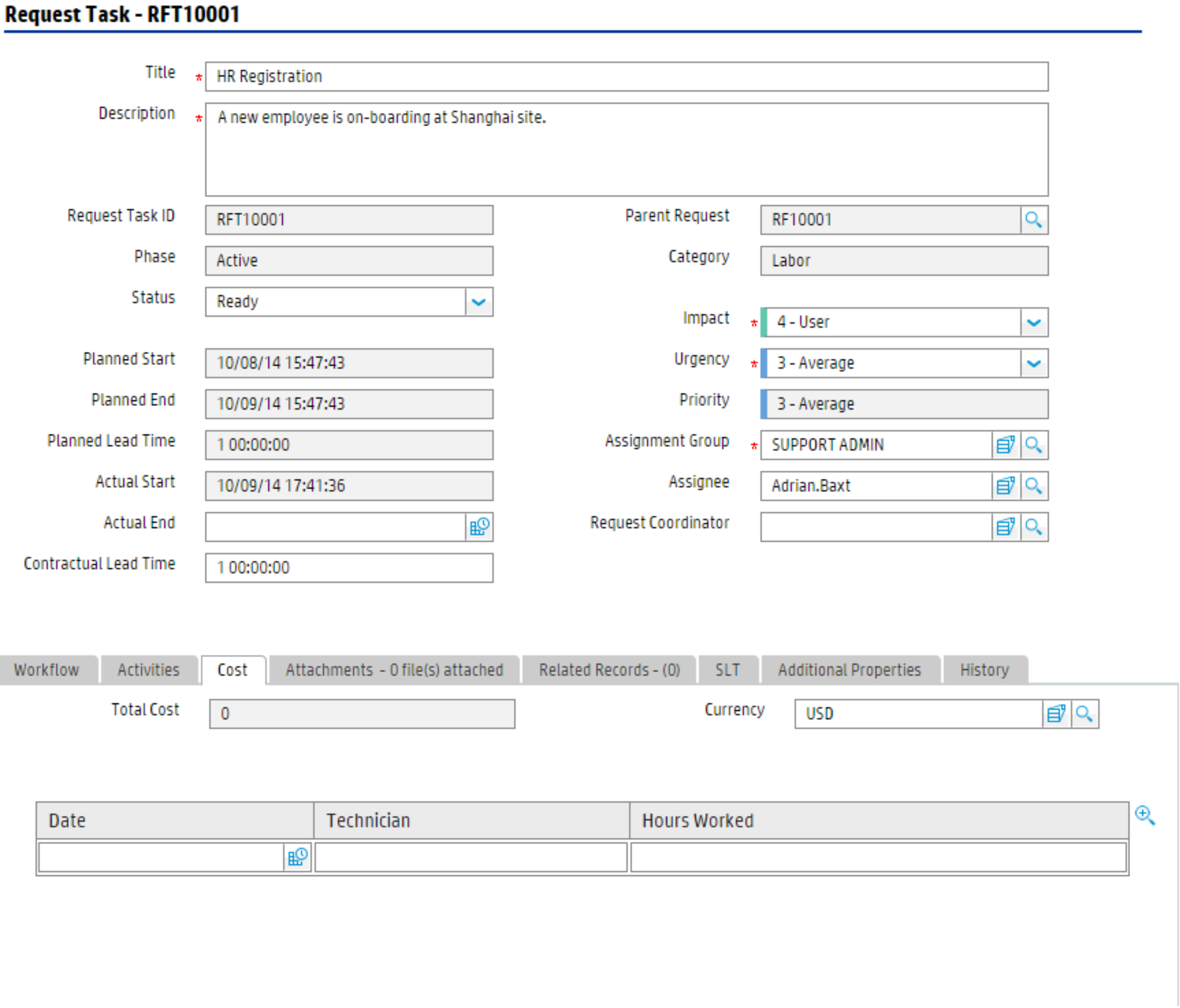
Label	Description
Related Records section	Contains a list of all related records for the request/order. The related records in request form include interactions, changes, incidents and requests. The related records in order form include interactions.
Approvals > Current Approvals	This subsection provides an overview of the current approvals related to request/order. The data displayed includes the following information: • Approval Type • Approval Status • # Approved • # Denied • # Pending
Approvals > Approval Log	This subsection provides an overview of the past approvals related to request/order. The data displayed includes the following information: • Action • Approver/Operator • By • Date/Time • Phase • ID
SLT section	The SLT (Service Level Target) section displays SLAs related to the request/order. The Service Level Targets subsection defines the Process Target details, such as beginning and ending state, and time allowed between these states. The Upcoming Alerts subsection displays the alerts to generate when processing the Process Target.
Tasks section	The planned/created request tasks are displayed in this section. Most of the tasks come from Request Model. However authorized operator (with “Edit Task Planner” right in “Request” area) is allowed to plan additional tasks via “Edit” button in the tasks section. To plan a new task, click the “Edit” button in tasks section, task editor is displayed for planning new tasks.

Request/Order field descriptions, continued

Label	Description
Task Context section	Displays the input and output parameters of all request tasks defined for the request/order.
History section	Displays the timestamps and operators that the request/order record is opened or updated by.

Request task forms

The following figure shows the common task form.



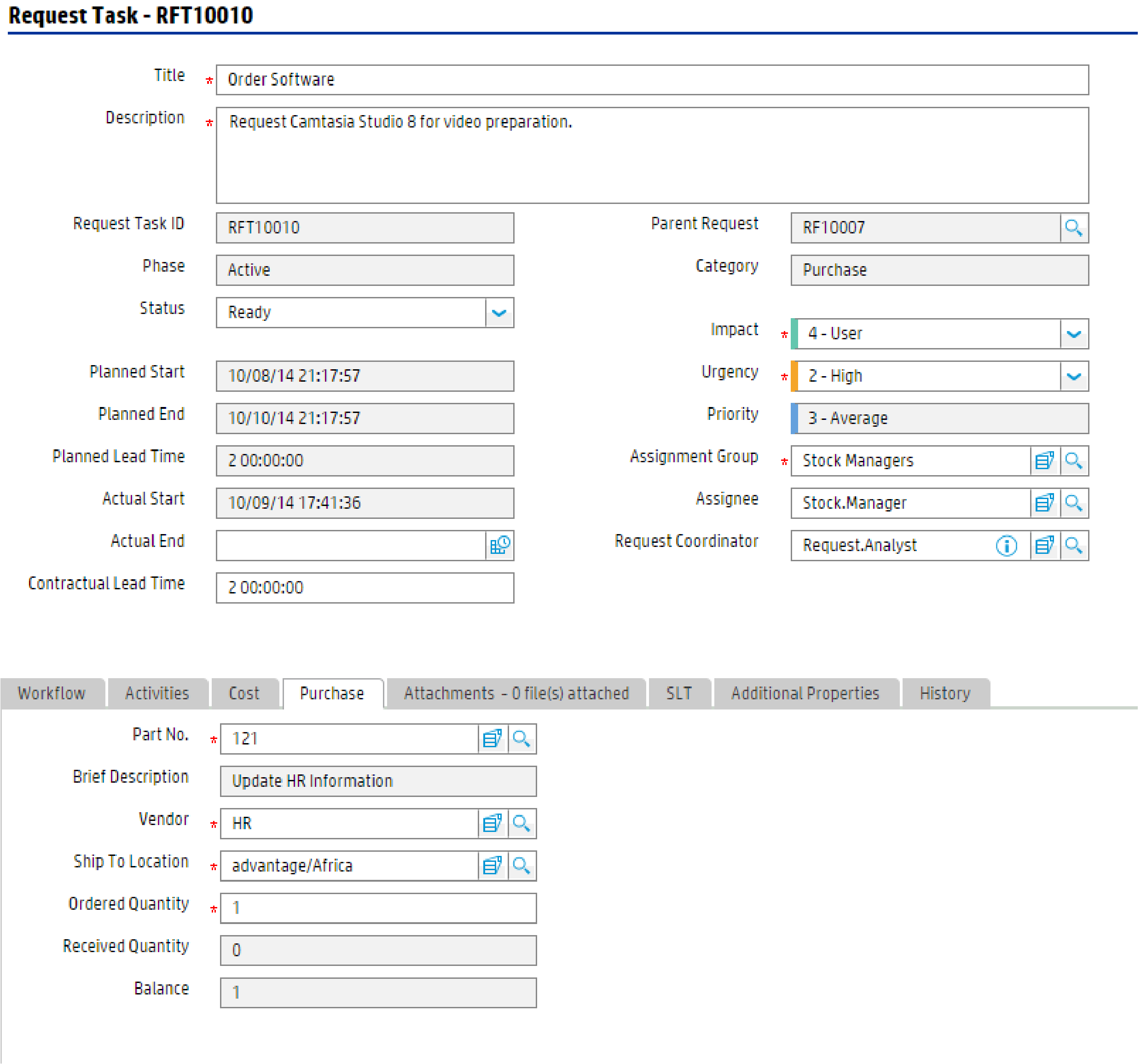
Request Task - RFT10001

Title *	HR Registration		
Description *	A new employee is on-boarding at Shanghai site.		
Request Task ID	RFT10001	Parent Request	RF10001
Phase	Active	Category	Labor
Status	Ready	Impact *	4 - User
Planned Start	10/08/14 15:47:43	Urgency *	3 - Average
Planned End	10/09/14 15:47:43	Priority	3 - Average
Planned Lead Time	1 00:00:00	Assignment Group *	SUPPORT ADMIN
Actual Start	10/09/14 17:41:36	Assignee	Adrian.Baxt
Actual End		Request Coordinator	
Contractual Lead Time	1 00:00:00		

Total Cost	0	Currency	USD

Date	Technician	Hours Worked

The following figure shows the purchase task form.



Request Task - RFT10010

Title * Order Software

Description * Request Camtasia Studio 8 for video preparation.

Request Task ID: RFT10010

Parent Request: RF10007

Phase: Active

Category: Purchase

Status: Ready

Impact * 4 - User

Urgency * 2 - High

Planned Start: 10/08/14 21:17:57

Priority: 3 - Average

Planned End: 10/10/14 21:17:57

Assignment Group * Stock Managers

Planned Lead Time: 2 00:00:00

Assignee: Stock.Manager

Actual Start: 10/09/14 17:41:36

Request Coordinator: Request.Analyst

Actual End:

Contractual Lead Time: 2 00:00:00

Part No. * 121

Brief Description: Update HR Information

Vendor * HR

Ship To Location * advantage/Africa

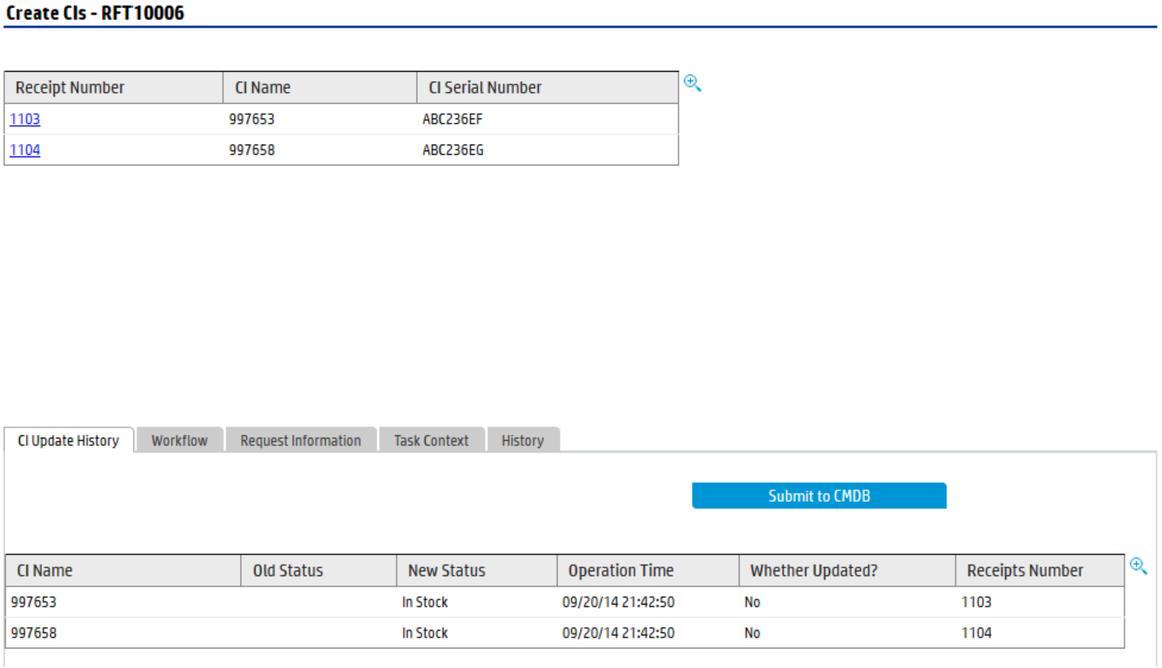
Ordered Quantity * 1

Received Quantity: 0

Balance: 1

The following figures show different CMDB update forms for different request task categories.

CMDB update form in “Purchase” task:

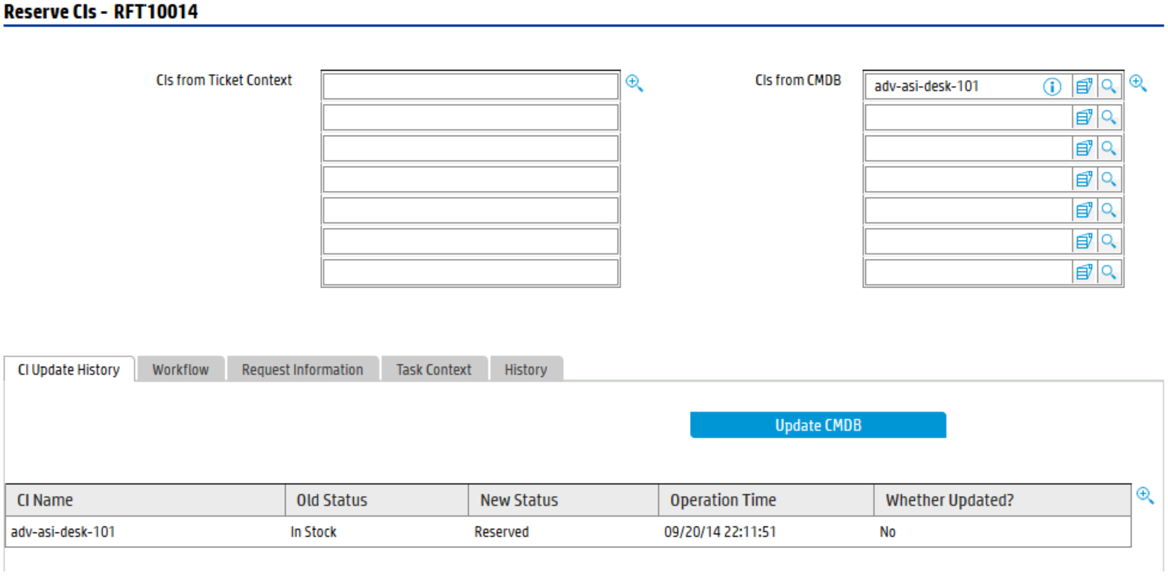


Create CIs - RFT10006

Receipt Number	CI Name	CI Serial Number
1103	997653	ABC236EF
1104	997658	ABC236EG

CI Name	Old Status	New Status	Operation Time	Whether Updated?	Receipts Number
997653		In Stock	09/20/14 21:42:50	No	1103
997658		In Stock	09/20/14 21:42:50	No	1104

CMDB update form in “Reservation” task:



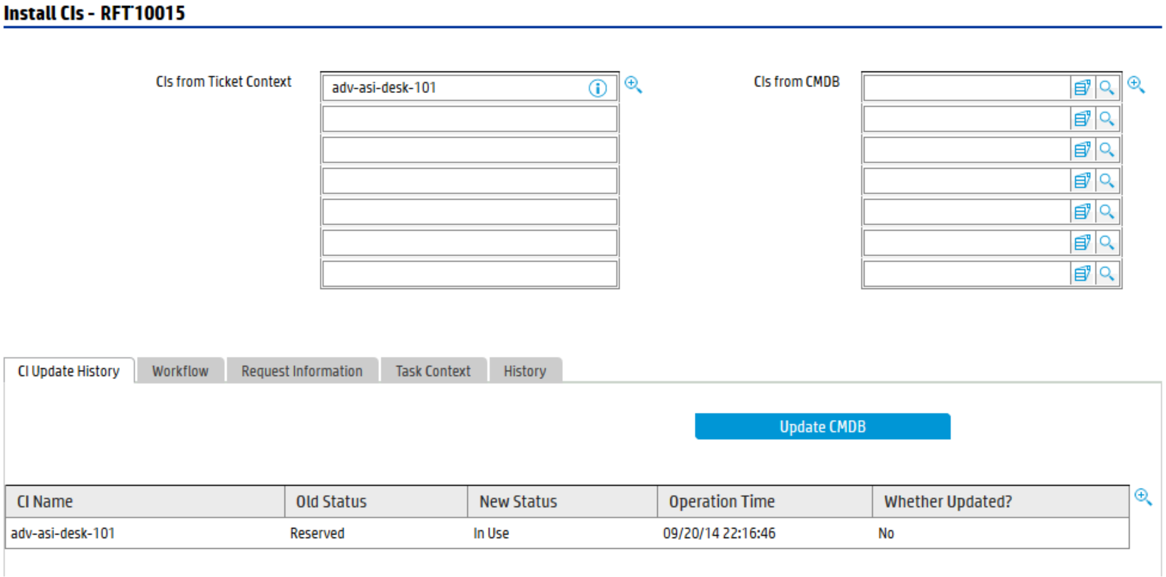
Reserve CIs - RFT10014

CIs from Ticket Context

CIs from CMDB: adv-asi-desk-101

CI Name	Old Status	New Status	Operation Time	Whether Updated?
adv-asi-desk-101	In Stock	Reserved	09/20/14 22:11:51	No

CMDB update form in “Installation” task:

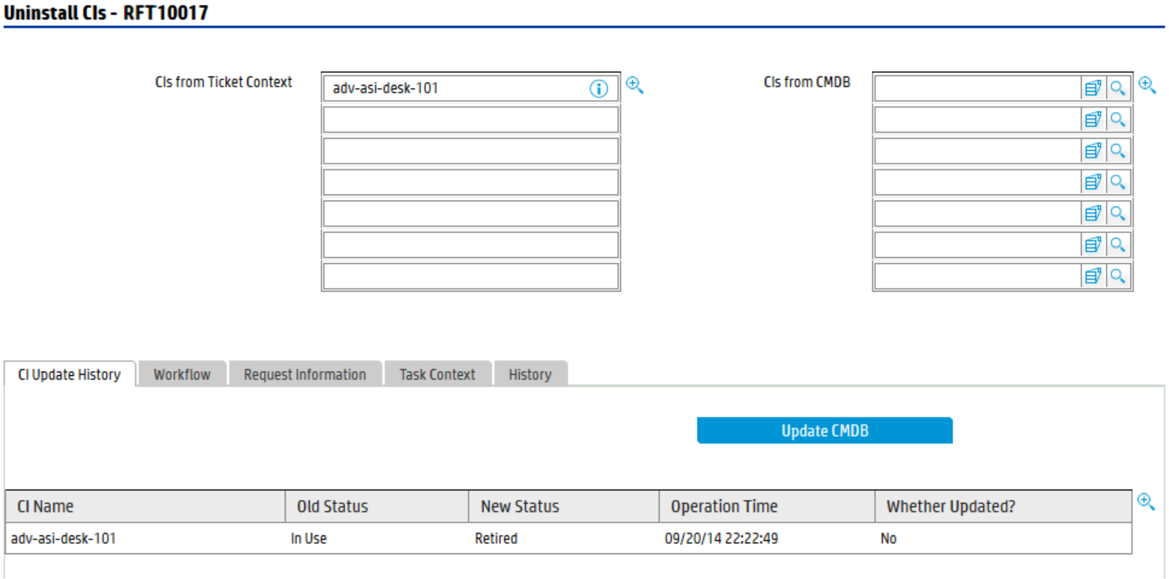


Install CIs - RFT10015

CIs from Ticket Context: adv-asi-desk-101

CI Name	Old Status	New Status	Operation Time	Whether Updated?
adv-asi-desk-101	Reserved	In Use	09/20/14 22:16:46	No

CMDB update form in “Uninstallation” task:

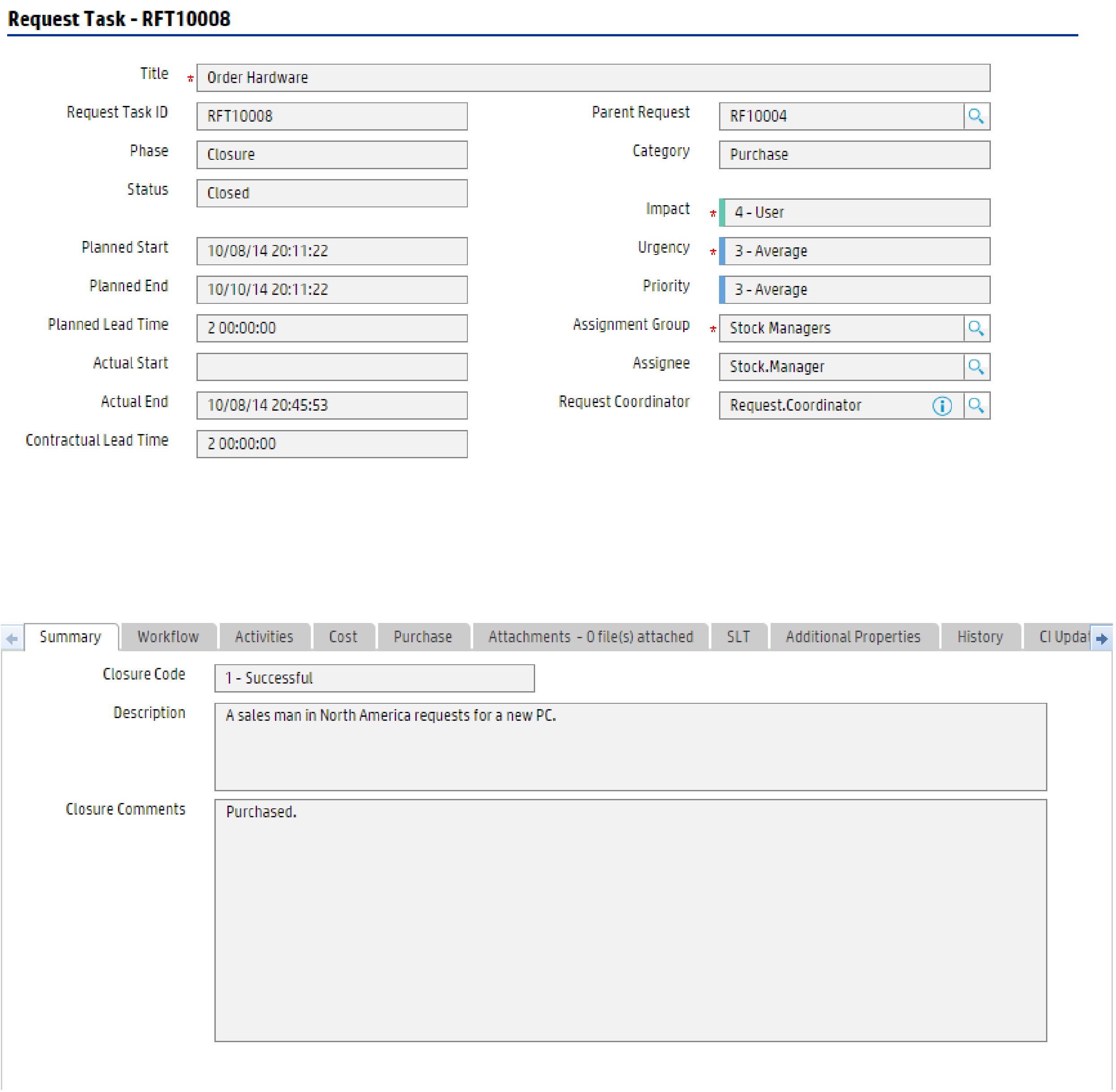


Uninstall CIs - RFT10017

CIs from Ticket Context: adv-asi-desk-101

CI Name	Old Status	New Status	Operation Time	Whether Updated?
adv-asi-desk-101	In Use	Retired	09/20/14 22:22:49	No

The following figure shows the closed request task form.



Request Task - RFT10008

Title *	Order Hardware		
Request Task ID	RFT10008	Parent Request	RF10004
Phase	Closure	Category	Purchase
Status	Closed		
		Impact *	4 - User
Planned Start	10/08/14 20:11:22	Urgency *	3 - Average
Planned End	10/10/14 20:11:22	Priority	3 - Average
Planned Lead Time	2 00:00:00	Assignment Group *	Stock Managers
Actual Start		Assignee	Stock.Manager
Actual End	10/08/14 20:45:53	Request Coordinator	Request.Coordinator
Contractual Lead Time	2 00:00:00		

Closure Code	1 - Successful
Description	A sales man in North America requests for a new PC.
Closure Comments	Purchased.

Request task form details

The following table identifies and describes some of the features on the request task form.

Request task field descriptions

Label	Description
Request Task ID	The system-generated unique ID for this request task.
Title	A short description that summarizes the request task. It is a mandatory field.
Description	A detailed description of the request task. This field is prepopulated with data from parent request/order. It is a mandatory field.
Parent Request	Displays the unique ID of parent request/order.
Category	This field describes the type of request task. In out-of-box, the following categories are available: • Automation • Installation • Labor • Purchase • Reservation • Uninstallation
Phase	This is a system-generated field that specifies the name of the current phase of the request task. These phases are available in out-of-box workflows: • Waiting • Active • Review • Closure • Cancelled • CMDB Update (only available in “Purchase”/“Reservation”/”Installation”/”Uninstallation” task workflow) • Execution (only available in “Automation” task workflow) • Completion (only available in “Automation” task workflow)
Status	Displays the status of the request task. These statuses are available in out-of-box workflows:

Request task field descriptions, continued

Label	Description
	• Planned – Request task is opened but not activated. • Ready – Request task is activated. • In Progress – Request task is being handled by Request Analyst. • Pending Customer – Additional information is required from user/requester. • Pending Vendor/Supplier – Vendor/Supplier will handle this request task. • CMDB Update (Only available in “Purchase”/“Reservation”/”Installation”/”Uninstallation” task workflow) – CMDB is being updated. • Pending Review – High priority request task will be reviewed. • Cancelled – Request task is cancelled. • Closed – Request task is closed.
Impact	A measure of the effect of the request task on business processes. Impact and urgency are used to assign priority. These impacts are available out-of-box: • Enterprise • Site/Dept • Multiple Users • User This field is prepopulated with data from parent request/order. It is a mandatory field.
Urgency	A measure of how long it will be until a request task has a significant impact on the business. Impact and urgency are used to assign priority. These urgencies are available out-of-box: • Critical • High • Average • Low

Request task field descriptions, continued

Label	Description
	This field is prepopulated with data from parent request/order. It is a mandatory field.
Priority	The order in which to address the request task in comparison to others. The priority value is calculated using impact and urgency.
Assignment Group	The support group assigned to work on this request task. This field can be prepopulated by the data defined in assignment rule or manually set by Request Coordinator. It is a mandatory field.
Assignee	The person assigned to work on this request task. This person is a member of the assignment group. This field can be prepopulated by the data defined in assignment rule or manually set by Request Coordinator.
Request Coordinator	The name of the person responsible for coordinating the implementation of the parent request/order. Each Coordinator may belong to several assignment groups. Each group can have just one Request Coordinator.
Planned Start	If “Global Lead Time” is not zero in request or order, this field will be calculated starting from request “Delivery Date” and upstream from the last task to the first one in task planner, task dependency and planned lead time will be considered. In case “Global Lead Time” is zero in request or order, this field will be calculated from the “Expected Finish Date” instead of “Delivery Date”. This field is read-only in the request task form.
Planned End	If “Global Lead Time” is not zero in request or order, this field will be calculated starting from request “Delivery Date” and upstream from the last task to the first one in task planner, task dependency and planned lead time will be considered. In case “Global Lead Time” is zero in request or order, this field will be calculated from the “Expected Finish Date” instead of “Delivery Date”. This field is read-only in the request task form.
Planned Lead Time	Defines the duration time that the request task will spend. Data is prepopulated by the value defined in task planner of Request Model. This field is read-only.
Actual Start	It will be auto-populated when task is activated.
Actual End	It will be manually filled by Request Analyst when request task is done.
Contractual Lead Time	By default it equals to “Planned Lead Time”. However it is allowed to be adjusted by authorized operator according to real situation. Once it is changed, the “Planned Start” and “Planned End” will be re-calculated accordingly. The out-of-box request task SLT is still measured based on “Planned Lead Time”.
Cost > Total Cost	Total cost incurred by fulfillment activities. This field in “Purchase” task indicates the cost of received part items. This field in other tasks indicates the labor cost.

Request task field descriptions, continued

Label	Description
Cost > Currency	Specifies the currency of the total cost.
Cost > Date/Technician/Hours Worked	The table specifies when and who will work on the request task for how many hours. The labor cost is calculated based on the hourly rate of the technician and the hours spent by the technician.
Purchase > Part No.	The part no. of the purchased item listed in product catalog. This is a required field.
Purchase > Vendor	The vendor of the specified part item which is defined in the modelvendor table. This is a required field.
Purchase > Ship To Location	The destination location the purchased items should be shipped to. This is a required field.
Purchase > Ordered Quantity	The number of part items requested or ordered. This is a required field.
Purchase > Received Quantity	The number of received part items.
Purchase > Balance	Equals “Ordered Quantity” minus “Received Quantity”.
CI Update History > button Submit to CMDB/Update CMDB	The Request Analyst clicks this button to execute actual CI creation or CI status update. A confirmation message box will be displayed once this button is clicked. If “Yes” is selected in the message box, CI will be created or CI status will be updated. Otherwise, CMDB update action is abandoned.
CI Update History > CI Name/Old Status/New Status/Operation Time/Whether Updated?/Receipts Number	Shows the CMDB update result. New created CIs will be shown in “Purchase” task. Status updated CIs will be shown in “Reservation”/“Installation”/”Uninstallation” task.
Request Information > CartItem Id/Cart Item/Requested For/Quantity/Status/User Selection	Displays the request information provided by user/requester. The request information includes the items ordered from Service Catalog, the user selection details of the ordered items. The information in this table will be referenced by the operator who performs CMDB update.
Summary > Closure Code	Specifies a predefined closure code to describe how the request task has been fulfilled. These closure codes are available out-of-box: • Successful • Successful (with problems)

Request task field descriptions, continued

Label	Description
	• Failed • Rejected (financial) • Rejected (technical) • Rejected (security) • Withdrawn • Withdrawal requested by customer • Cancelled • Denied request fulfillment
Summary > Closure Comments	This field is to document additional comments to close the request task.
Workflow section	Displays a figure of request task workflow. It indicates the current phase which the request task is in, and traces the phase transition history.
Activities section	Records information that the operator enters during the lifecycle of the request task. Every time you update a request task, you can fill in an update on the Activities section (New Update) with or without “Visible to Customer” flagged. A log of all the updates is stored on the Journal Updates and activities list.
Attachments section	You can use the Attachments section to attach documents to request task.
Related Records section	Contains a list of all related records for the request task. The related records in request task form only include changes.
SLT section	The SLT (Service Level Target) section displays SLAs related to the request task. The Service Level Targets subsection defines the Process Target details, such as beginning and ending state, and time allowed between these states. The Upcoming Alerts subsection displays the alerts to generate when processing the Process Target.
Task Context section	Displays the input and output parameters of the request task.
History section	Displays the timestamps and operators that the request task is opened or updated by.

Chapter 22: Service Level Management Overview

You can use Service Level Management (SLM) to improve the quality of services that you provide to customers. You can also use Service Level Management to quantify the financial benefits in reduced incidents, outages, and time invested in system failures and downtime. Service Level Management collects performance information automatically to track service guarantees. Service Level Management enables you to achieve the following results:

- Ensure compliance with service and process targets set in the Service Level Agreement
- Report performance information to track the effectiveness and efficiency of managed services
- Detect and track failures of service guarantees
- Quantify costs associated with planned and unplanned service outages

Service Level Management uses the Service Level Targets (SLTs) to measure operational activities in other HP Service Manager applications .

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

Topics in this section include:

"Service Level Management within the ITIL Framework" below

"Service Level Management Application" on the next page

"Input and output for Service Level Management" on the next page

"Key performance indicators for Service Level Management" on page 344

"Service Level Management Roles" on page 345

"RACI matrix for Service Level Management" on page 347

Service Level Management within the ITIL Framework

The Service Level Management process is described in ITIL’s Service Design publication.

The document describes Service Level Management as a vital process for every IT Service to document Service Level Targets and responsibilities within Service Agreements. The purpose of the SLM process is to ensure that all IT Services are delivered to agreed and achievable targets.

By using Service Level Management in HP Service Manager each IT Service Provider has a consistent interface to the business for all service level related data. The business gets up to date information about performance against the agreed service level targets. The operational teams are aligned to the agreed service targets, which will help to reduce breached targets. For breached targets, SLM provides the underlying data to facilitate the analysis of the cause of breaches. SLM provides the required tools to facilitate the prevention of breaches from re-occurrence. Furthermore, SLM provides reliable documentation features to efficiently communicate with the business .

Service Level Management Application

The impetus for a robust Service Level Management system is delivering value to the business by improving the quality of service , reduced number of incidents, and increased customer satisfaction. Over time, you can quantify the financial benefits in reduced incidents, outages, and time invested in system failures and downtime. The time and money recovered can be invested in improved customer relationships, more sophisticated monitoring, better training, and improved business efficiency.

Service management best practices describe the goals for Service Level Management (SLM) as follows:

The goal for SLM is to maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring and reporting upon IT Service achievements and instigation of actions to eradicate poor service—in line with business or cost justification. Through these methods, a better relationship between IT and its customers can be developed.

HP Service Manager supports these goals by providing a service management best practices compliant application framework with a built-in workflow. The primary Service Level Management goals are the following:

- Tracking of Service Targets for Service and CIs, which includes planned and unplanned outages
- Proactive tracking of Process Targets, which tracks the amount of time it takes for the incident, service desk interaction, or change request to advance to the next state (For example, the amount of time required for an incident record status to change from Open to Work in Progress.)

Configuring Service Level Targets within SLA, OLAs or UCs, are the supporting elements which help Service Level Management to accomplish these goals.

Input and output for Service Level Management

A number of sources are relevant for the Service Level Management process.

Input	Output
Business information: from the organization’s business strategy, plans, and financial plans and information on their current and future requirements	Service reports: providing details of the service levels achieved in relation to the targets contained within SLAs. These reports should contain details of all aspects of the service and its delivery, including current and historical performance, breaches and weaknesses, major events, changes planned, current and predicted workloads, customer feedback, and improvement plans and activities
Business Impact Analysis: providing information on the impact, priority, risk and number of users associated with each service	Service Improvement Plan (SIP): an overall program or plan of prioritized improvement actions, encompassing all services and all processes, together with associated impacts and risks
Business requirements: details of any agreed, new or changed business requirements	The Service Quality Plan (SQP): documenting and planning the overall improvement of service quality
The strategies, policies and constraints from Service Strategy	Service Level Agreements (SLAs): a set of targets and responsibilities should be documented and agreed within an SLA for each operational service
The Service Portfolio and Service Catalog	Service Level Requirements (SLRs): a set of targets and responsibilities should be documented and agreed within an SLR for each proposed new or changed service.
Change information: from the Change Management process with a forward schedule of changes and a need to assess all changes for their impact on all services	Operational Level Agreements (OLAs): a set of targets and responsibilities should be documented and agreed within an OLA for each internal support team
CMS: containing information on the relationships between the business services, the supporting services and the technology	Reports on OLAs and underpinning contracts
Customer and user feedback, complaints and compliments	Service review meeting minutes and actions: all meetings should be scheduled on a regular basis, with planned agendas and their discussions and actions recorded and progressed
Information and input from any of the other processes (for example, Incident Management, Capacity Management, and Availability Management), together with the existing SLAs, SLRs, and OLAs and past service reports on the quality of service delivered.	SLA review and service scope review meeting minutes: summarizing agreed actions and revisions to SLAs and service scope Revised contracts: changes to SLAs or new SLRs may require existing underpinning contracts to be changed, or new contracts to be negotiated and agreed.

Key performance indicators for Service Level Management

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

Title	Description
% of SLAs / OLAs / UCs that meet expectations	This KPI gives the user the ability to review the SLAs, OLAs and UCs, which met their target.
% of breached SLAs / OLAs / UCs	This KPI gives the user the ability to review the SLAs, OLAs and UCs, which did not met their target.

ITIL recommended KPIs

- Percentage reduction in SLA targets missed
- Percentage reduction in SLA targets threatened
- Percentage increase in customer perception and Satisfaction of SLA achievements, via service reviews and Customer Satisfaction Survey responses
- Percentage reduction in SLA breaches caused because of third-party support contracts (underpinning contracts)
- Percentage reduction in SLA breaches caused because of internal Operational Level Agreements (OLAs).

Deliver service as previously agreed at affordable costs:

- Total number and percentage increase in fully documented SLAs in place
- Percentage increase in SLAs agreed against operational services being run
- Percentage reduction in the costs associated with service provision
- Percentage reduction in the cost of monitoring and reporting of SLAs

- Percentage increase in the speed of developing and agreeing appropriate SLAs
- Frequency of service review meetings.

Manage business interface:

- Increased percentage of services covered by SLAs
- Documented and agreed SLM processes and procedures are in place
- Reduction in the time taken to respond to and implement SLA requests
- Increased percentage of SLA reviews completed on time
- Reduction in the percentage of outstanding SLAs for annual renegotiation
- Reduction in the percentage of SLAs requiring corrective changes (for example, targets not attainable; changes in usage levels). Care needs to be taken when using this KPI
- Percentage increase in the coverage of OLAs and third-party contracts in place, whilst possibly reducing the actual number of agreements (consolidation and centralization)
- Documentary evidence that issues raised at service and SLA reviews are being followed up and resolved
- Reduction in the number and severity of SLA breaches
- Effective review and follow-up of all SLA, OLA and underpinning contract breaches.

Service Level Management Roles

Role	Responsibilities
Service Level Management Process Owner	• Accountable for the definition, management, governance and improvement of the Service Level Management Process • Ensures that the Service Level Management process and working practices are effective and efficient • Ensures that all stakeholders are sufficiently involved in the Service Level Management process • Ensures that (business) management is sufficiently informed as to the volume, impact and cost of SLAs, OLAs and UCs

Role	Responsibilities
	• Ensures tight linkage between the Service Level Management process and other related processes
Service Level Manager	• Ensures that the customer's current and future Service requirements are identified, understood and documented in SLAs and SLRs • Drafts and ensures sign off of the SDD • Negotiates and agrees on the levels of Service to be delivered with the customer (either internal or external); formally documenting these levels of Service in SLAs • Negotiates and agrees to OLAs and, in some cases, other SLAs and agreements that underpin the SLAs • Ensures that targets agreed to within Underpinning Contracts are aligned with SLA and SLR targets • Ensures that Service Performance Reviews are regularly performed, and any required actions are performed • Ensures that improvement initiatives identified in Service Reviews are acted on and progress reports are provided to customers
Service Owner	• Provides the correct relationship information for the Services and CIs in the Service Catalog • Reports any discrepancies in the Service Catalog details and the actual environment into the Service Catalog maintenance process • Provides input for Service Catalog maintenance process improvement
Supplier Manager	• Produces requests for proposal in cooperation with all the stakeholders (Service Level Manager, Business Manager, etc) • Selects suppliers based on the evaluation of proposal they supply and feedback from stakeholders • Drafts and negotiates SLAs, Contracts, Agreements or any other documents for Third-Party Suppliers • Ensures the targets agreed within contracts are aligned with SLR targets • Ensures that SLA breaches of each supplier are highlighted, investigated and action(s) taken to prevent their recurrence
Service Level Analyst	• Ensures that Service reports are produced for each customer Service • Performs gap analysis to highlight breaches of SLA targets, investigating reasons and recommending actions to prevent their recurrence

Role	Responsibilities
	- Plans and schedules the Service Performance Review meetings and document the results and actions
Support Groups	Implement improvement initiatives identified in Service Reviews
Customer	Responsible for the purchase of goods or Services
User	Consumes goods or services

RACI matrix for Service Level 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. The RACI matrix for Service Level Management is shown in the table below.

Process ID	Activity	Service Level Manager	Supplier Manager	Service Owner	Customer	Service Level Analyst	Resolver Groups
SD 2.1	Maintain the Service Catalog	A/R		C	C		
SD 2.2	Create or Amend IT Services	A/R	R	R	C		
SD 2.3	Draft Supporting Agreements	A/R	R	R			
SD 2.4	Finalise SLAs / OLAs / UCs	A/R	R	R	C/I		
SD 2.5	Monitor Service Levels	A/R	I	I	C		
SD 2.6	Service Level Reporting	A/R				R	
SD 2.7	Perform Service Reviews	A/R			C	R	
SD 2.8	Service Improvement Programme	A/R		R	C		R
SD 2.9	Review / Revise SLA / OLA / UC	A/R				R	

Chapter 23: Service Level Management Workflows

The Service Level Management process includes all necessary steps to create and maintain Service offerings including the management of the following items:

- Service Level Agreements between business and IT
- Operational Level Agreements between IT and IT
- Underpinning contracts between IT and external providers.

In addition, Service Level management process includes the activities such as:

- Service Level Reporting, including measurement of the service performance
- Production of service reports
- Conduction of service reviews with identification of improvement opportunities documented in the SIP or SQP
- The assessment of customer satisfaction with logging of complaints and compliments

The Service Level Management process can consist of following activities:

"Updating the Service Catalog (SD 2.1)" on page 350

"Create or Amend IT Services (SD 2.2)" on page 351

"SLRs and draft OLAs and UCs (SD 2.3)" on page 353

"Finalize SLRs/OLAs/UCs (SD 2.4)" on page 356

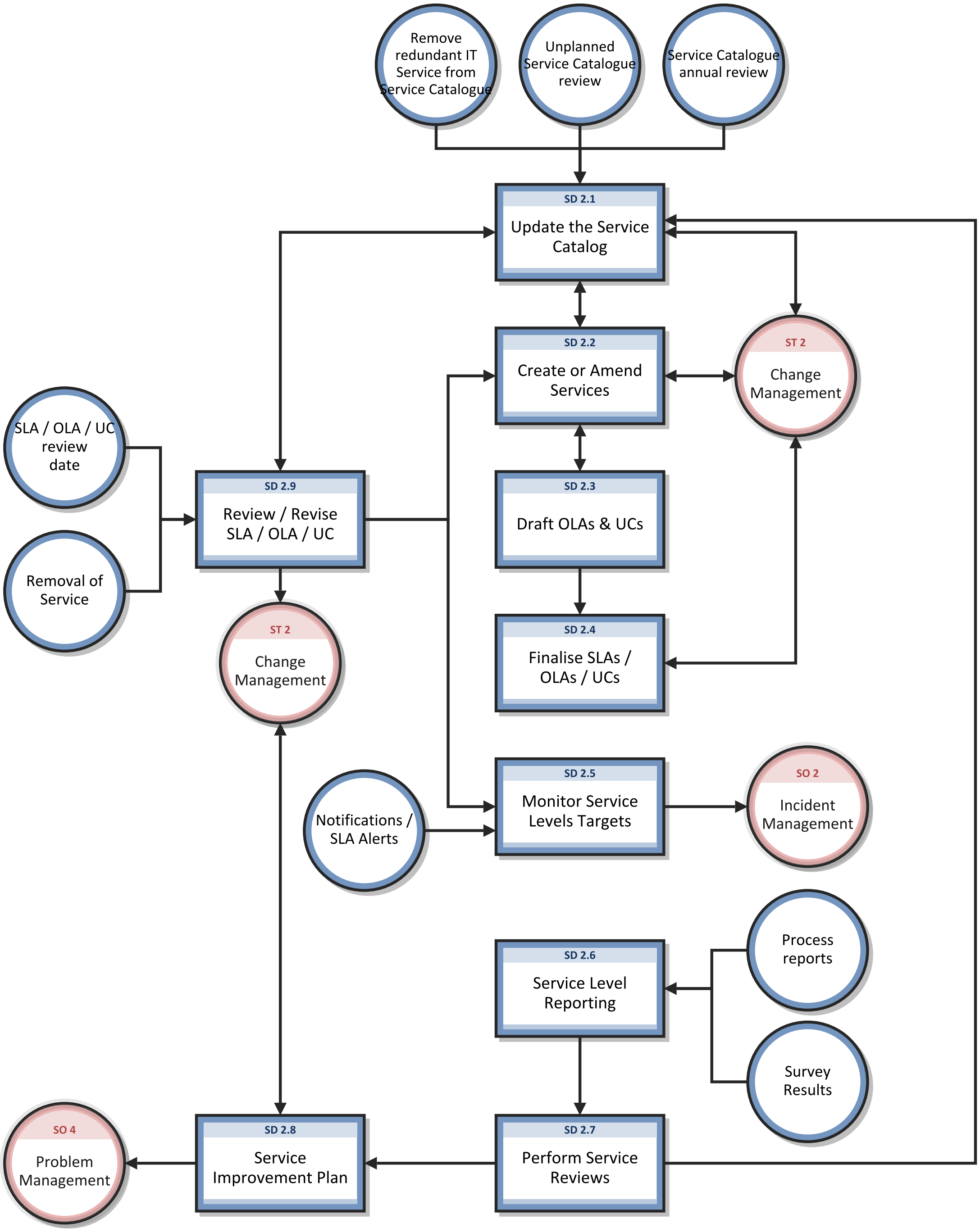
"Monitor Service Levels (SD 2.5)" on page 357

"Service Level Reporting (SD 2.6)" on page 360

"Perform Service Reviews (SD 2.7)" on page 361

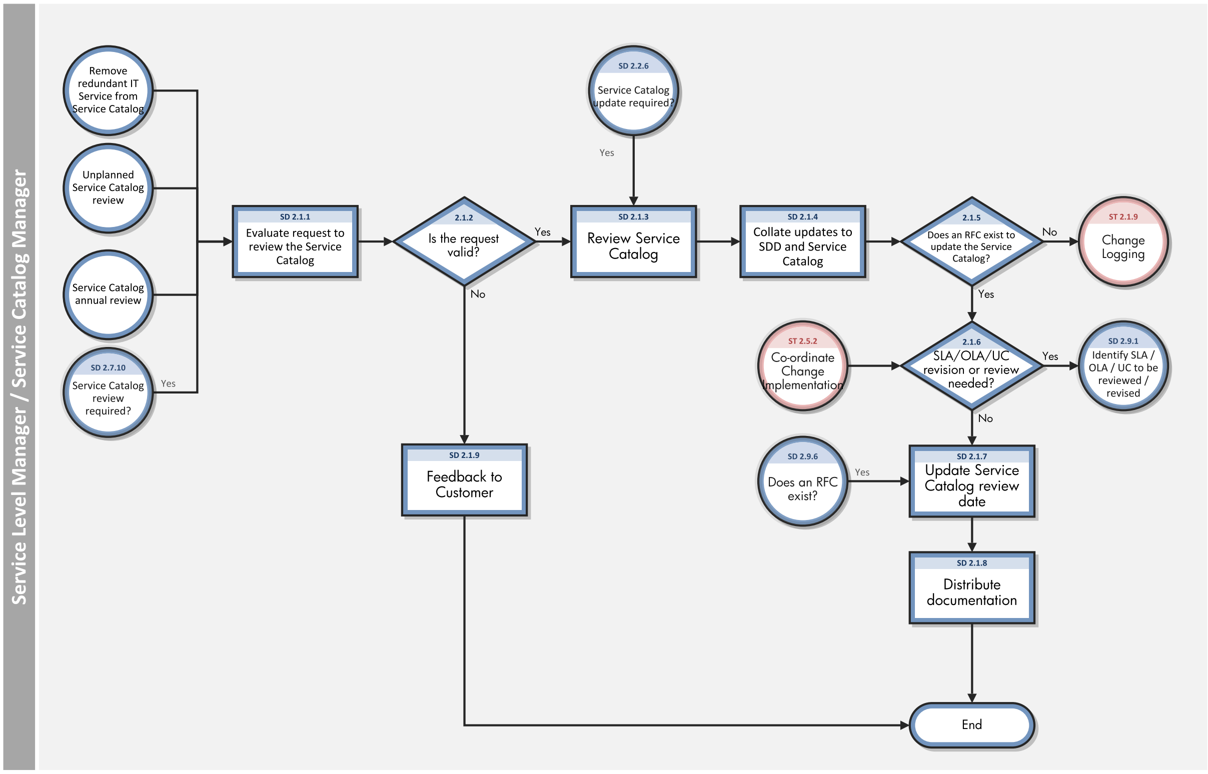
"Service Improvement Plan (SD 2.8)" on page 364

"Review and Revise SLAs/OLAs/UCs (SD 2.9)" on page 367


Remove redundant IT Service from Service Catalogue
Unplanned Service Catalogue review
Service Catalogue annual review
SD 2.1
Update the Service Catalog
SD 2.2
Create or Amend Services
ST 2
Change Management
SLA / OLA / UC review date
SD 2.9
Review / Revise SLA / OLA / UC
SD 2.3
Draft OLAs & UCs
Removal of Service
ST 2
Change Management
SD 2.4
Finalise SLAs / OLAs / UCs
SD 2.5
Monitor Service Levels Targets
SO 2
Incident Management
Notifications / SLA Alerts
Process reports
SD 2.6
Service Level Reporting
Survey Results
SO 4
Problem Management
SD 2.8
Service Improvement Plan
SD 2.7
Perform Service Reviews

Updating the Service Catalog (SD 2.1)

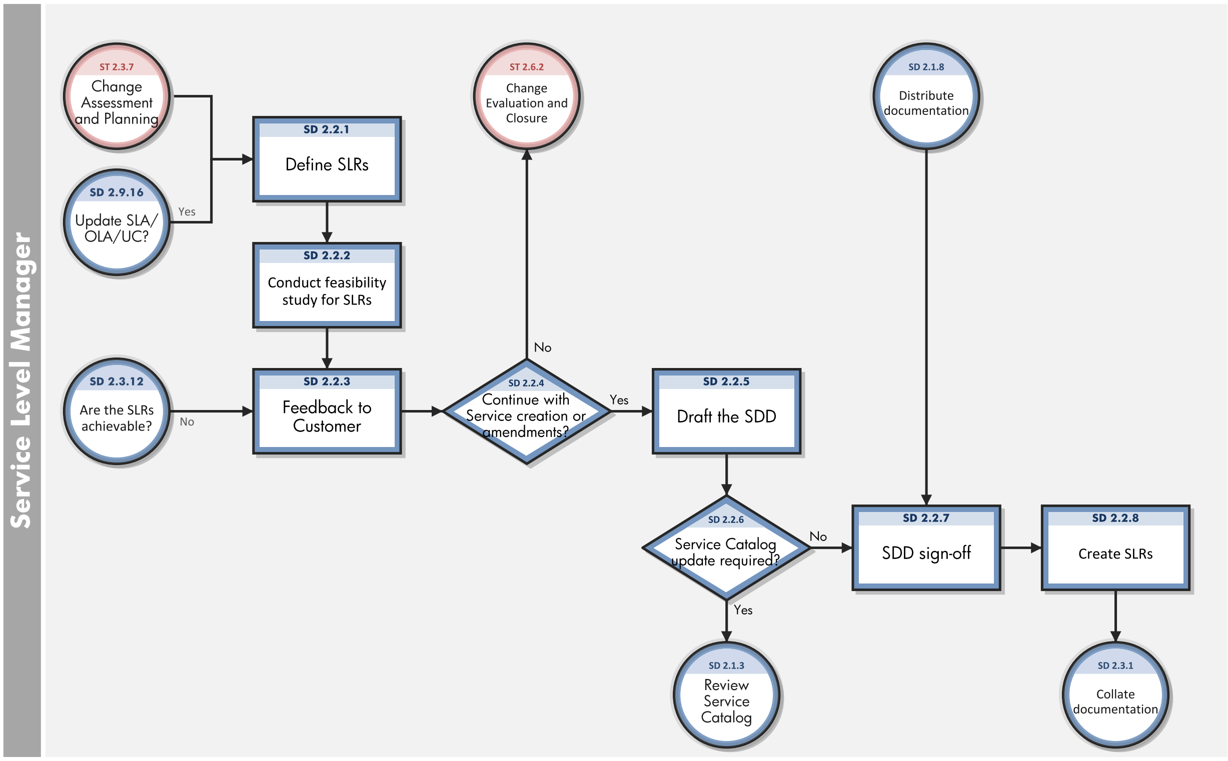
Process ID	Procedure or Decision	Description	Role
SD 2.1.1	Evaluate request to review the Service Catalog	The Service Level Manager reviews the request and any relevant information to determine whether or not the request is valid. Go to SD 2.1.2 to determine whether the request is valid.	Service Level Manager
SD 2.1.2	Is the request valid?	If yes, go to SD 2.1.3 to review the Service Catalog. If no, go to SD 2.1.9 to feedback to the Customer.	Service Level Manager
SD 2.1.3	Review Service Catalog	Determine what changes may be required to the Service Catalog and SDD. The Service Owner and Customer may be involved in the review. Go to SD 2.1.4 to collate updates to the SDD and Service Catalog.	Service Level Manager
SD 2.1.4	Collate updates to SDD and Service Catalog	Compile updates to the SDD and Service Catalog. Go to SD 2.1.5 to determine whether an RFC exists.	Service Level Manager
SD 2.1.5	Does an RFC exist to update the Service Catalog?	If yes, go to SD 2.1.6 to determine whether the SLA / OLA / UC need to be revised or reviewed. If no, go to Change Logging (ST 2.1.9) to create a new Change record.	Service Level Manager
SD 2.1.6	SLA / OLA / UC Revision or review needed?	If yes, go to SD 2.9.1 to identify any agreements to be reviewed and/or revised. If no, go to SD 2.1.7 to update the Service Catalog review date.	Service Level Manager
SD 2.1.7	Update Service Catalog review date	Update the Service Catalog to show that it has been reviewed and record the next scheduled review date. Go to SD 2.1.8 to distribute documentation.	Service Level Manager
SD 2.1.8	Distribute documentation	Once the RFC to change the Service Catalog has been confirmed as successful, the new documents (including the SDD and Service Catalog) are circulated to the relevant stakeholders. The Maintain the Service Catalog process ends.	Service Level Manager
SD 2.1.9	Feedback to Customer	The customer is advised that the request to amend the Service Catalog is not valid and provided with the reason. The Maintain the Service Catalog process ends.	Service Level Manager


Service Level Manager / Service Catalog Manager
Remove redundant IT Service from Service Catalog
Unplanned Service Catalog review
Service Catalog annual review
SD 2.7.10
Service Catalog review required?
Yes
SD 2.1.1
Evaluate request to review the Service Catalog
2.1.2
Is the request valid?
Yes
No
SD 2.2.6
Service Catalog update required?
Yes
SD 2.1.3
Review Service Catalog
SD 2.1.4
Collate updates to SDD and Service Catalog
2.1.5
Does an RFC exist to update the Service Catalog?
No
Yes
ST 2.1.9
Change Logging
ST 2.5.2
Co-ordinate Change Implementation
2.1.6
SLA/OLA/UC revision or review needed?
Yes
No
SD 2.9.1
Identify SLA / OLA / UC to be reviewed / revised
SD 2.9.6
Does an RFC exist?
Yes
SD 2.1.7
Update Service Catalog review date
SD 2.1.8
Distribute documentation
SD 2.1.9
Feedback to Customer
End

Create or Amend IT Services (SD 2.2)

Process ID	Procedure or Decision	Description	Role
SD 2.2.1	Define SLRs	Once a request is received for a new or amended IT Service, determine and agree the main requirements of the business. Go to SD 2.2.2 to conduct a feasibility study for the Service Level Requirements.	Service Level Manager
SD 2.2.2	Conduct feasibility study for SLRs	Initiate a feasibility study, ensuring that any existing OLAs and UCs are taken into consideration. The Supplier Manager may be involved with Service Providers if necessary. The study must consider all elements including technology, cost and Serviceability. Go to SD 2.2.3 to feedback to the Customer.	Service Level Manager
SD 2.2.3	Feedback to Customer	The results of the feasibility study are fed back to the Customer. Go to SD 2.2.4 to determine whether to continue with the	Service Level Manager

Process ID	Procedure or Decision	Description	Role
		Service creation or amendments.	
SD 2.2.4	Continue with Service creation or amendments?	If yes, go to SD 2.2.5 to draft the SDD. If no, go to Change Evaluation and Closure (ST 2.6.2) to close the Change.	Service Level Manager
SD 2.2.5	Draft the SDD	Draft the SDD based on the data gathered and validated in the requirements definition and feasibility study. The SDD covers: • a description of the business process concerned • a detailed description of the technology and support platforms • links to related policies and Service Management procedures • plans to monitor and measure the Service Go to SD 2.2.6 to determine whether a Service Catalog update is required.	Service Level Manager
SD 2.2.6	Service Catalog update required?	If yes, go to SD 2.1.10 to review the Service Catalog. If no, go to SD 2.2.7 to sign-off the SDD.	Service Level Manager
SD 2.2.7	SDD sign-off	Validate the SDD with the Customer and then sign-off with the Service Owner and Service Level Manager. Once signed off, update the Service Catalog to reflect the new or amended Service. Go to SD 2.2.8 to finalize the SLRs.	Service Level Manager
SD 2.2.8	Create SLRs	The SLRs are created by the Service Level Manager and the Customer and are then collated into the SLR document.	Service Level Manager

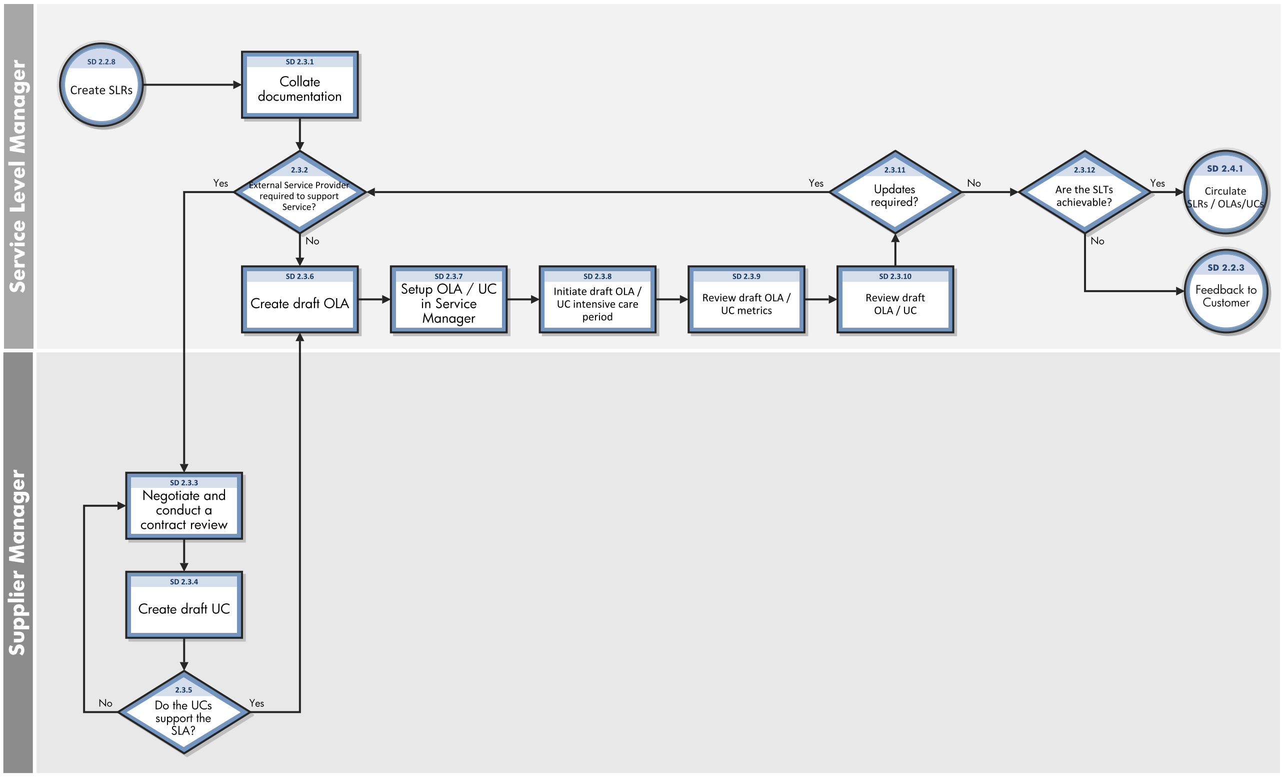


SLRs and draft OLAs and UCs (SD 2.3)

Process ID	Procedure or Decision	Description	Role
SD 2.3.1	Collate documentation	Compile supporting documentation such as existing OLAs and UCs, the Service Catalog, the SDD and SLRs documents. Go to SD 2.3.2 to determine whether the Service Provider is required to support the Service.	Service Level Manager
SD 2.3.2	External Service Provider required to support Service?	If yes, go to SD 2.3.3 to negotiate with the Service Provider and conduct a contract review. If no, go to SD 2.3.6 to create the draft OLA.	Service Level Manager
SD 2.3.3	Negotiate and conduct a contract review.	Contact the Service Provider(s) to discuss how the SLRs will be supported. If contracts are already in place it may not be possible to renegotiate, and this will need to be taken into account when the SLA is drafted.	Supplier Manager

Process ID	Procedure or Decision	Description	Role
		Go to SD 2.3.4 to create the draft UC.	
SD 2.3.4	Create draft UC	The UC is drafted following the contract review and negotiation. Go to SD 2.3.5 to determine whether the UCs support the SLA.	Supplier Manager
SD 2.3.5	Do the UCs support the SLA?	If the UCs do support the SLRs, go to SD 2.3.6 to create the draft OLA. If no, go to SD 2.3.3 to continue negotiation and contract review.	Supplier Manager
SD 2.3.6	Create draft OLA	Review the SLRs, the SDD and the Service Catalog to determine the requirements for the OLA with the Service Owner or Supplier Manager. Determine the OLA intensive care start date and duration. Go to SD 2.3.7 to setup the OLA/UC in Service Manager.	Service Level Manager
SD 2.3.7	Setup OLA / UC in Service Manager	The Service Level Manager will ensure that the OLA / UC is set up in Service Manager by liaising with the Service Manager Admin team. Go to SD 2.3.8 to initiate the draft OLA / UC intensive care period.	Service Level Manager
SD 2.3.8	Initiate draft OLA / UC intensive care period	Monitor the performance of the OLA / UC against the draft OLA / UC metrics using data from other processes, such as Incident and Problem Management. Go to SD 2.3.9 to review the draft OLA / UC metrics.	Service Level Manager
SD 2.3.9	Review draft OLA / UC metrics	Once the OLA intensive care period is complete, conduct a Service Review meeting to: • determine if achievement meets expectations of the draft OLA / UC • determine whether the SLTs in the SLRs are achievable • determine whether the draft OLA / UC are ‘fit for purpose’ • identify amendments to the draft OLAs / UCs prior to converting these into formal OLA / UC metrics • identify gaps between the required Service and current Service capabilities and consider additional resource requirements to bridge them Go to SD 2.3.10 to review the draft OLA / UC.	Service Level Manager

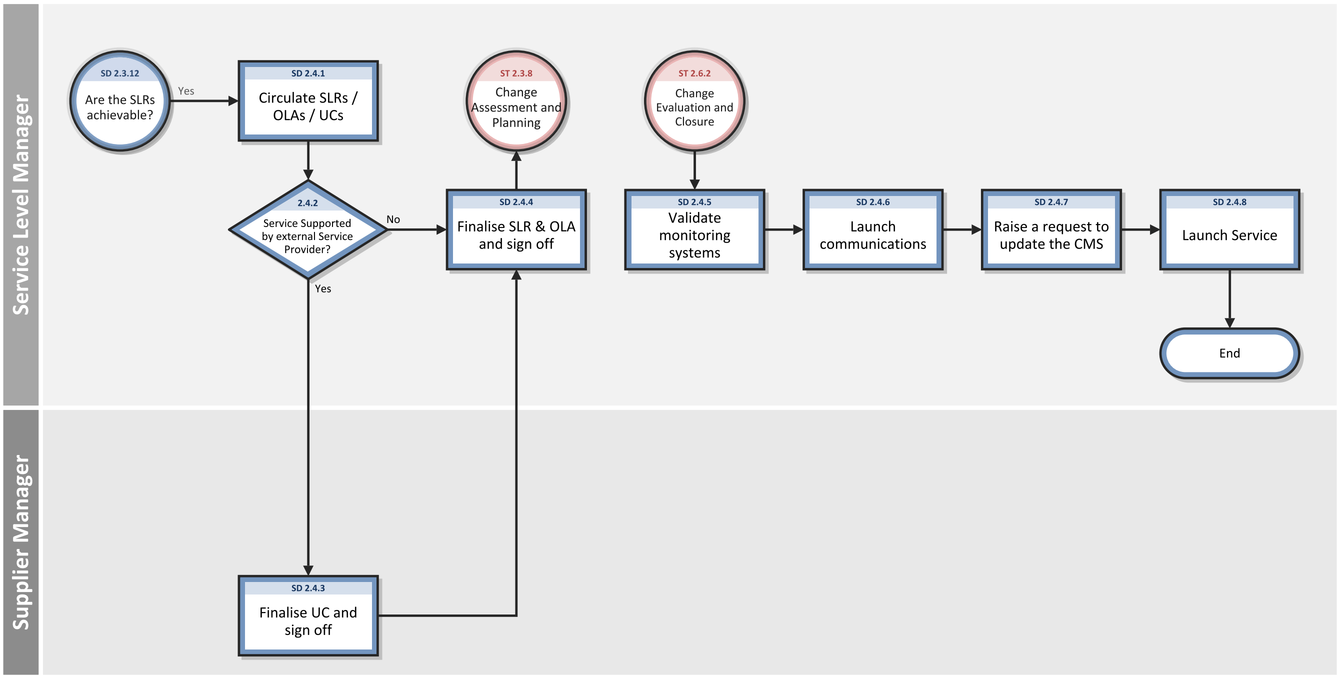
Process ID	Procedure or Decision	Description	Role
SD 2.3.10	Review draft OLA / UC	The drafts OLAs / UCs are reviewed to ensure they meet the requirements and support the new SLRs. Go to SD 2.3.11 to determine whether updates are required.	Service Level Manager
SD 2.3.11	Updates required?	If updates are required to the draft agreements based on the review, go to SD 2.3.2 to repeat the process If no, go to SD 2.3.12 to determine whether the SLTs in the SLRs are achievable.	Service Level Manager
SD 2.3.12	Are the SLTs achievable?	If yes, go SD 2.4.1 to circulate the draft agreements. If no, go to SD 2.2.3 to feedback to the customer.	Service Level Manager



Finalize SLRs/OLAs/UCs (SD 2.4)

Process ID	Procedure or Decision	Description	Role
SD 2.4.1	Circulate SLRs / OLAs / UCs	The SLRs, OLAs and UCs are circulated to the relevant audience as pre-reading before the final confirmation and sign off meeting. Go to SD 2.4.2 to determine whether the Service will be supported by a Service Provider.	Service Level Manager
SD 2.4.2	Service supported by an external Service Provider?	If yes, go to SD 2.4.3 finalize and sign off the UC. If no, go to SD 2.4.4 to finalize the SLR and OLA, and sign off.	Service Level Manager
SD 2.4.3	Finalize UC and sign off	The UCs are finalized to ensure they can support the SLR and are signed off by the Supplier Manager and the Service Provider. Go to SD 2.4.4 to finalize and sign-off the SLR and OLA.	Supplier Manager
SD 2.4.4	Finalize SLR & OLA and sign-off	The Service Level Manager finalizes and signs off the SLR and OLA with the Customer, Service Owner and Supplier Manager. As part of the SLR discussion a launch date for the Service is agreed which takes into account how much time is needed to update the Service and the Service Manager. Go to Change Assessment and Planning (ST 2.3.8) to plan and schedule the SLA and OLA Change. The Finalize SLRs / OLAs / UCs process is temporarily stopped pending implementation of the Change.	Service Level Manager
SD 2.4.5	Validate monitoring systems	Once the Change has been confirmed as successful, the monitoring systems are re-validated to ensure they accurately monitor and manage the service level targets. Go to SD 2.4.6 to launch communications.	Service Level Manager
SD 2.4.6	Launch communications	Initiate communications to the end-user community and the delivery teams, including the Service Desk. Go to SD 2.4.7 to raise a request to update the CMS.	Service Level Manager
SD 2.4.7	Raise a request to update the CMS	Raise a request to update the CMS for the new or amended Service. Go to SD 2.4.8 to launch the Service.	Service Level Manager
SD 2.4.8	Launch Service	The Service is launched and the following elements become "Live":	Service Level

Process ID	Procedure or Decision	Description	Role
		• Agreed Service Level parameters automated in the Service Management system • Monitoring of Service delivery through the Service Management system The Finalize SLAs/OLAs/UCs process ends.	Manager

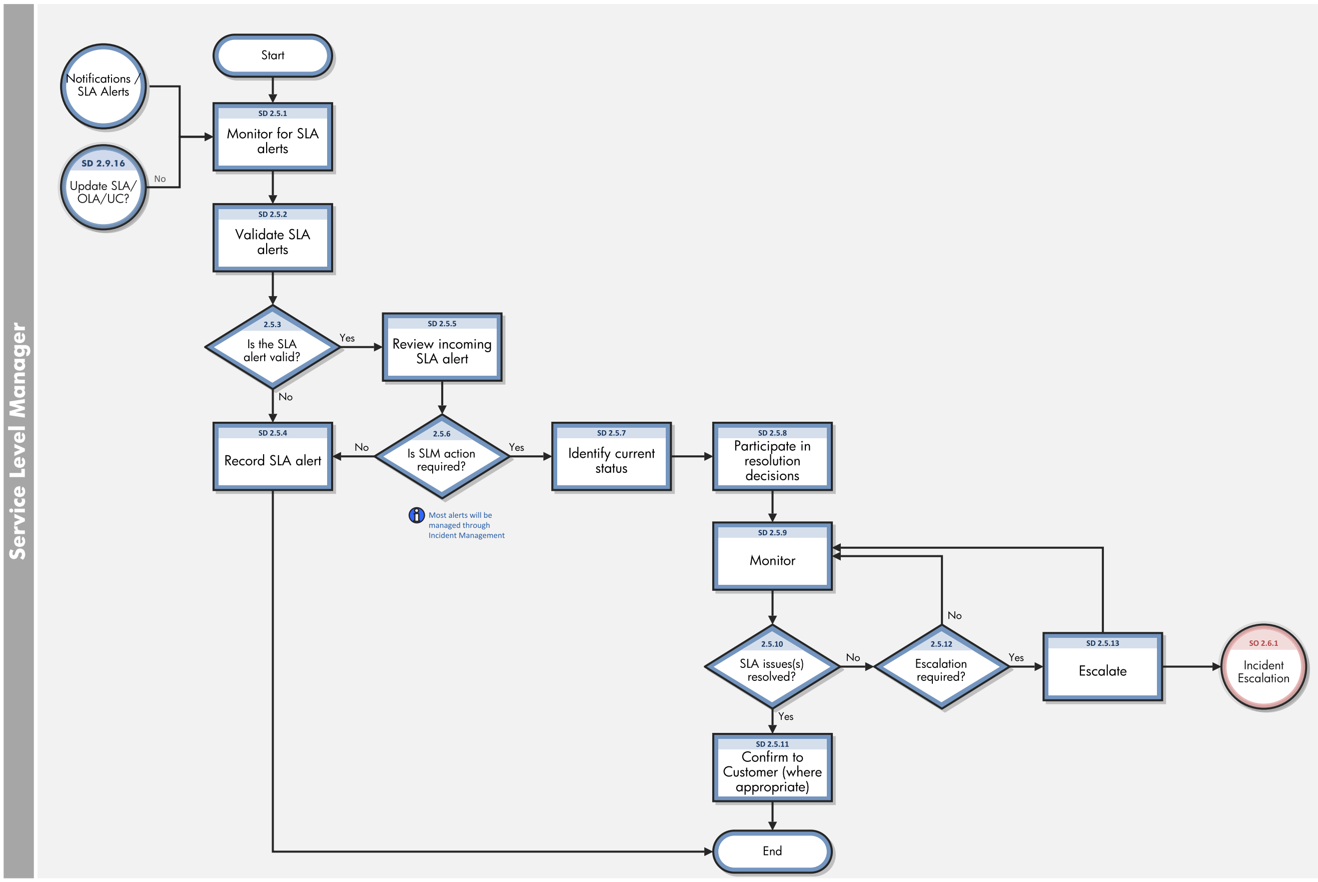

Service Level Manager
Supplier Manager
SD 2.3.12
Are the SLRs achievable?
Yes
SD 2.4.1
Circulate SLRs / OLAs / UCs
2.4.2
Service Supported by external Service Provider?
No
Yes
ST 2.3.8
Change Assessment and Planning
ST 2.6.2
Change Evaluation and Closure
SD 2.4.4
Finalise SLR & OLA and sign off
SD 2.4.5
Validate monitoring systems
SD 2.4.6
Launch communications
SD 2.4.7
Raise a request to update the CMS
SD 2.4.8
Launch Service
End
SD 2.4.3
Finalise UC and sign off

Monitor Service Levels (SD 2.5)

Process ID	Procedure or Decision	Description	Role
SD 2.5.1	Monitor for SLA alerts	The majority of day-to-day issues will be handled by the Service Desk and those Service Providers involved in delivering the Service/s. The SLM team will be notified of significant breaches of Service Level targets,that is, urgent P1 and major Incidents. Go to SD 2.5.2 to validate SLA alerts.	Service Level Manager
SD 2.5.2	Validate SLA alerts	Once an automated SLA alert is received its validity / relevance is assessed with agreed escalation points contained within the SLA. Go to SD 2.5.3 to determine whether the SLA alert is valid.	Service Level Manager

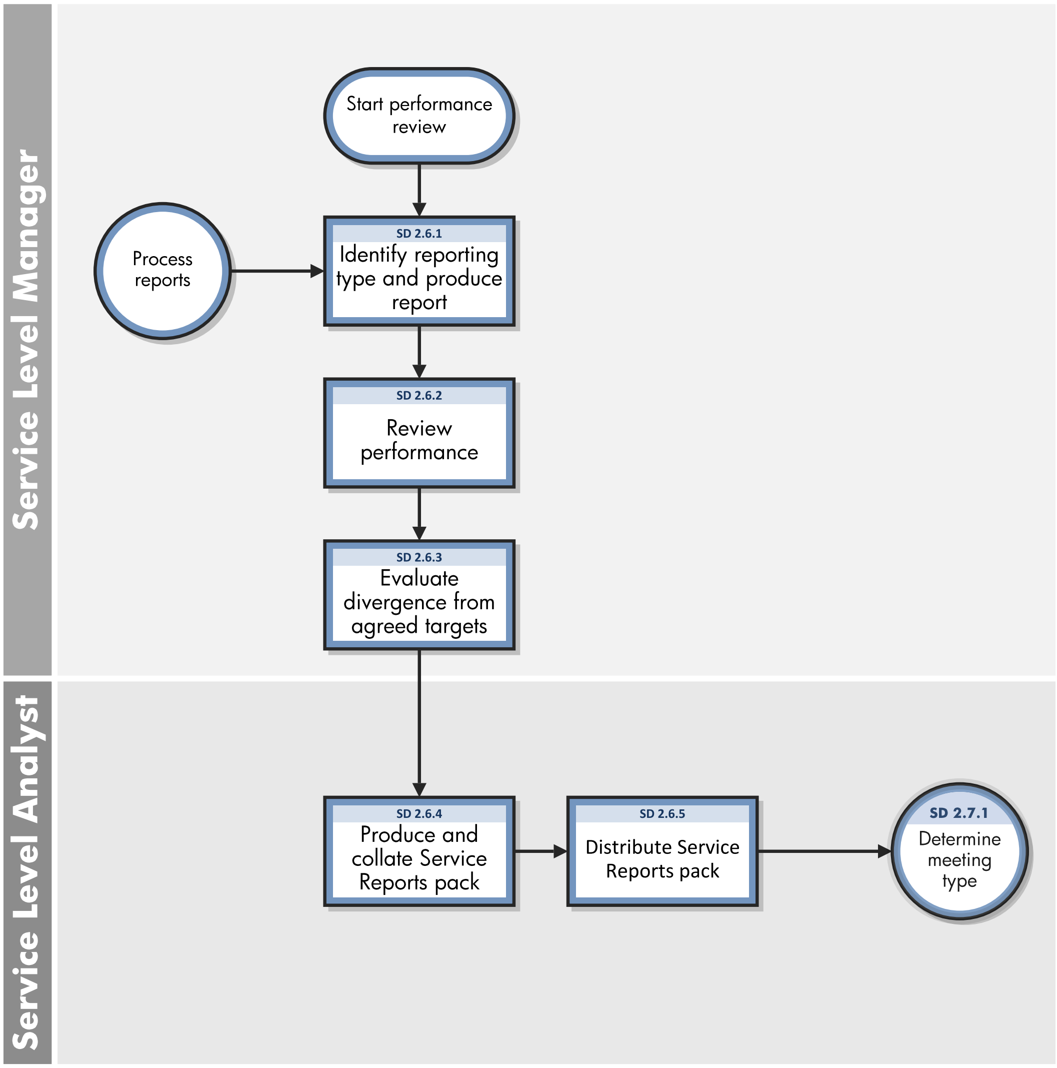
Process ID	Procedure or Decision	Description	Role
SD 2.5.3	Is the SLA alert valid?	If yes, go to SD 2.5.5 to review the incoming SLA alert. If no, go to SD 2.5.4 to record the SLA alert.	Service Level Manager
SD 2.5.4	Record SLA alert	The Service Level Manager records the invalid SLA Alert for future review of alert criteria. The Monitor Service Levels process ends.	Service Level Manager
SD 2.5.5	Review incoming SLA alert	The SLA alert is reviewed to determine: • associated Service and SLA • importance level of escalation • Incident/Problem/Major Incident record number • Support groups Go to SD 2.5.6 to determine whether SLA action is required.	Service Level Manager
SD 2.5.6	Is SLM action required?	If yes, go to SD 2.5.7 to identify the current SLA alert status. If no, go to SD 2.5.4 to record the SLA alert.	Service Level Manager
SD 2.5.7	Identify current status	Gather additional information about the current status of the Incident generating the alert. Go to SD 2.5.8 to participate in resolution decisions.	Service Level Manager
SD 2.5.8	Participate in resolution decisions	The Service Level Manager participates in decisions regarding the ongoing management of the Incident and possible resolution activities. This ensures that the Customer is kept informed of progress against the SLA and that the Service Owners and Service Providers are kept aware of the ongoing impact to the business. Go to SD 2.5.9 to monitor the Incident.	Service Level Manager
SD 2.5.9	Monitor	Periodically review the Incident to ensure that progress is being made and that agreed actions have been completed. Go to SD 2.5.10 to determine whether the SLA issue(s) is resolved.	Service Level Manager
SD 2.5.10	SLA Issue(s) resolved?	If the reason for the SLA alert has been resolved, go to SD 2.5.11 to confirm with the Customer (where appropriate). If no, go to SD 2.5.12 to determine whether escalation is required.	Service Level Manager

Process ID	Procedure or Decision	Description	Role
SD 2.5.11	Confirm to Customer (where appropriate)	Confirm the resolution with the Customer. The Monitor Service Levels process ends.	Service Level Manager
SD 2.5.12	Escalation required?	If yes, go to SD 2.5.13 to perform Incident escalation. If no, go to SD 2.5.9 to monitor the Incident.	Service Level Manager
SD 2.5.13	Escalation	If the performance is nearing its target, the Incident should be escalated via Incident Management. Go to Incident Escalation (SO 2.6.1) to determine how to resolve the Incident.	Service Level Manager



Service Level Reporting (SD 2.6)

Process ID	Procedure or Decision	Description	Role
SD 2.6.1	Identify reporting type and produce report	Reporting requirements are identified and reports produced based on: • Service metrics • SLAs • Service Catalog • Service Improvement updates Go to SD 2.6.2 to review	Service Level Manager
SD 2.6.2	Review performance	Review metrics available for Service Performance, including Incident resolution and response times. The metrics are validated for accuracy. Go to SD 2.6.3 to evaluate divergence from agreed targets.	Service Level Manager
SD 2.6.3	Evaluate divergence from agreed targets	The metrics are compared to the service targets for each live SLA. Go to SD 2.6.4 in order for the Service Level Analyst to produce and collate the Service Reports pack.	Service Level Manager
SD 2.6.4	Produce and collate Service Reports pack	Record findings and document within the Service Reports pack according to the structure agreed within the SLA. Go to SD 2.6.5 to distribute the Service Reports pack.	Service Level Analyst
SD 2.6.5	Distribute Service Reports pack	The completed Service Report packs are distributed to the Service Level Managers and Customers. Go to SD 2.7.1 in order for the Service Level Manager to determine the meeting type for the Service Review.	Service Level Analyst

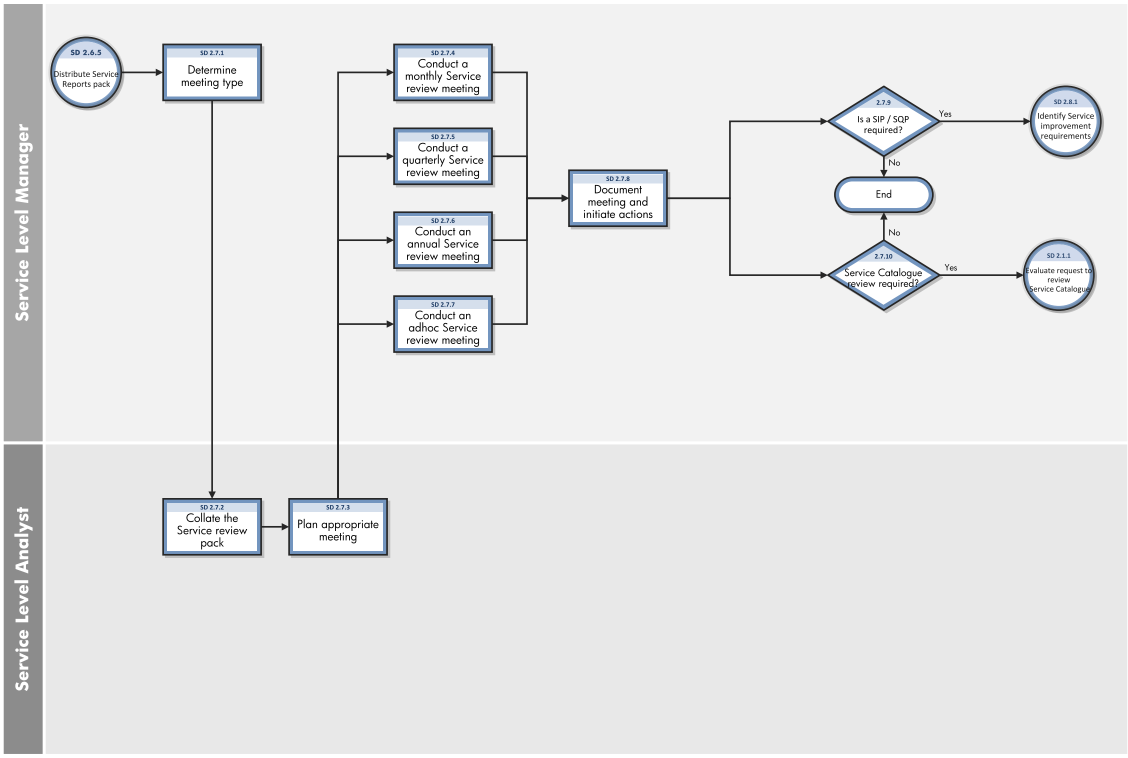


Perform Service Reviews (SD 2.7)

Process ID	Procedure or Decision	Description	Role
SD 2.7.1	Determine meeting type	Determine the appropriate meeting type from the agreed meeting schedule. Go to SD 2.7.2 to collate the Service review pack.	Service Level Manager
SD 2.7.2	Collate the Service	Collate the Service review pack, including:	Service Level

Process ID	Procedure or Decision	Description	Role
	review pack	• Meeting agenda • Previous minutes and outstanding actions • Service metrics • SIP progress • Informal and ad-hoc Customer feedback Key inputs should also be obtained from other Service Management processes and related documents. Go to SD 2.7.3 to plan the appropriate meeting.	Analyst
SD 2.7.3	Plan appropriate meeting	Determine whether the Service review is a monthly, quarterly, annual or ad-hoc meeting. Set the date and location of meeting and circulate the agenda to the appropriate audience. Go to one of the appropriate steps: • SD 2.7.4 to conduct a monthly Service Review meeting • SD 2.7.5 to conduct a quarterly Service Review meeting • SD 2.7.6 to conduct an annual Service Review meeting • SD 2.7.7 to conduct an ad-hoc Service Review meeting	Service Level Analyst
SD 2.7.4	Conduct a monthly Service review meeting	The purpose of this meeting is to understand and manage operational issues. The Customer and Service Level Manager will discuss: • requests for new and amended Services • updates to existing Service provision • progress on ongoing SIPs • Changing business requirements which may impact the current IT Services provided Go to SD 2.7.8 to document the meeting and initiate actions.	Service Level Manager
SD 2.7.5	Conduct a quarterly Service review meeting	This meeting follows the same agenda as the monthly Service Review meeting but with an additional item to cover more strategic issues. Go to SD 2.7.8 to document the meeting and initiate actions.	Service Level Manager

Process ID	Procedure or Decision	Description	Role
SD 2.7.6	Conduct an annual Service review meeting	This meeting is specifically designed to review the overall operation of the IT Service Management process in conjunction with the Customer. This will be an opportunity to review the SLAs that are included in the Service review pack allowing all parties to re-confirm that the IT Services are meeting the Customer's requirements and to discuss any future SLRs. Go to SD 2.7.8 to document the meeting and initiate actions.	Service Level Manager
SD 2.7.7	Conduct an adhoc Service review meeting	Both the Service Level Manager and Customer are entitled to call an ad-hoc Service Review meeting without having to wait for the next scheduled Service Review, in order to cover specific issues that may have arisen. Go to SD 2.7.8 to document the meeting and initiate actions.	Service Level Manager
SD 2.7.8	Document meeting & initiate actions	Document and issue minutes. There are 2 parallel activities from this activity. Go to SD 2.7.9 to determine whether a Service Improvement Plan (SIP) is required. Go to SD 2.7.10 to determine whether a Service Catalog review is required.	Service Level Manager
SD 2.7.9	Is an SIP/SQP required?	If yes, go to SD 2.8.1 to identify Service improvement requirements. If no, the Perform Service Reviews process ends.	Service Level Manager
SD 2.7.10	Service Catalog review required?	If yes, go to SD 2.1.1 to evaluate the request to review the Service Catalog. If no, the Perform Service Reviews process ends.	Service Level Manager

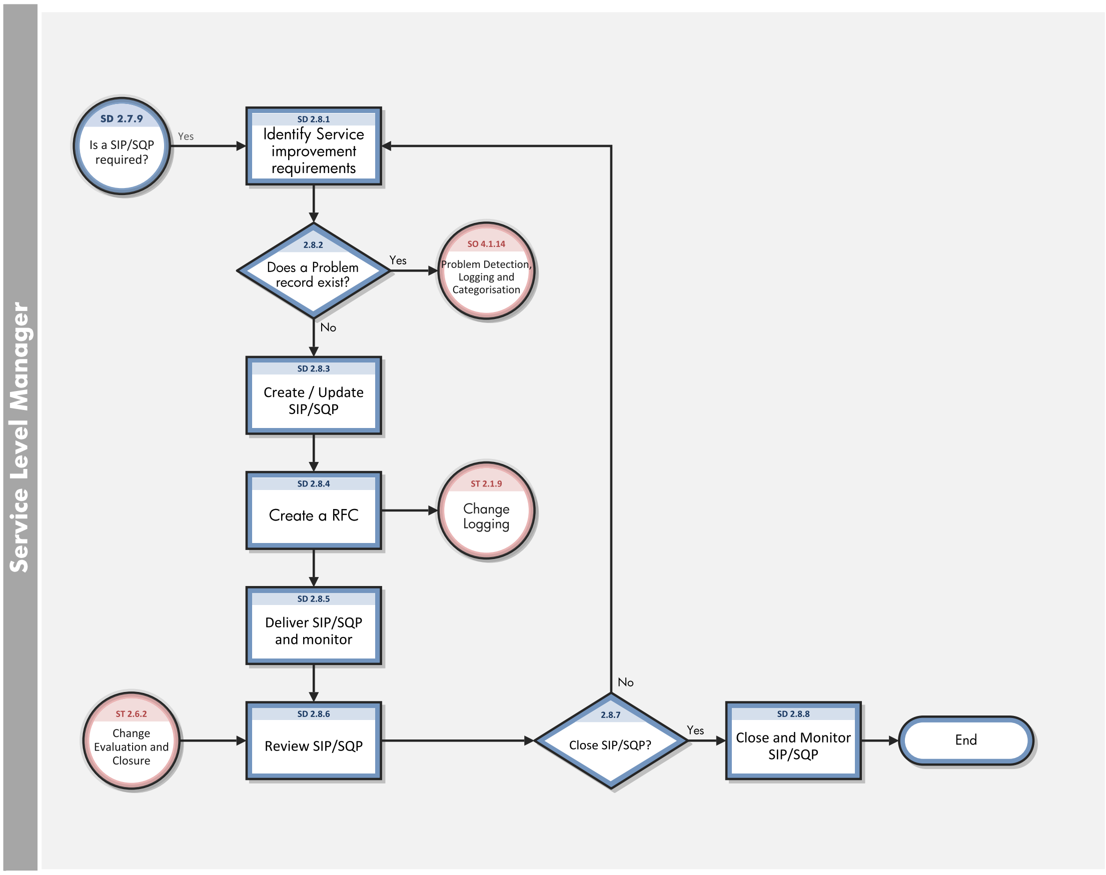

Service Level Manager
Service Level Analyst
SD 2.6.5
Distribute Service Reports pack
SD 2.7.1
Determine meeting type
SD 2.7.2
Collate the Service review pack
SD 2.7.3
Plan appropriate meeting
SD 2.7.4
Conduct a monthly Service review meeting
SD 2.7.5
Conduct a quarterly Service review meeting
SD 2.7.6
Conduct an annual Service review meeting
SD 2.7.7
Conduct an adhoc Service review meeting
SD 2.7.8
Document meeting and initiate actions
2.7.9
Is a SIP / SQP required?
Yes
No
End
No
2.7.10
Service Catalogue review required?
Yes
SD 2.8.1
Identify Service improvement requirements
SD 2.1.1
Evaluate request to review Service Catalogue

Service Improvement Plan (SD 2.8)

Process ID	Procedure or Decision	Description	Role
SD 2.8.1	Identify Service improvement requirements	Various inputs are used to establish the underlying requirement, such as: • Service Review data • Process Review data • Service and process reports • SLA monitoring • Problem Management • Customer Satisfaction The Service Level Manager will create a team to assist with requirement identification which includes Service Level Management, Problem Management, Customer satisfaction	Service Level Manager

Process ID	Procedure or Decision	Description	Role
		results and any relevant technical or process personnel. The Complaints and Compliments, Problem and Known Error database is checked to ensure the issues are not being dealt with already. Go to SD 2.8.2 to determine whether a Problem record exists.	
SD 2.8.2	Does a Problem record exist?	If yes, go to Problem Detection, Logging and Categorization (SO 4.1.14) to determine the related outstanding Problem. If no, go to SD 2.8.3 to develop an SIP/SQP plan.	Service Level Manager
SD 2.8.3	Create / Update an SIP/SQP	The creation of an SIP/SQP must include CSFs and measurement KPIs to assess whether targets are being met. The following people should be involved in discussion and agreement of the SIP/SQP: • Customer • Service Owner • Service Level Manager • Relevant support groups An SIP/SQP Program Board may be created and includes the following people: • Service Owner • Service Level Manager • Delivery team senior management The Program Board agrees on the composition of the team and appoints an SIP/SQP Program Manager. Go to SD 2.8.4 to create an RFC.	Service Level Manager
SD 2.8.4	Create an RFC	There are 2 parallel activities following this process step. An RFC should be submitted to support the new SIP. Go to Change Logging (ST 2.1.8) to create a new Change and go to SD 2.8.5 to deliver the SIP and monitor progress.	Service Level Manager
SD 2.8.5	Deliver SIP/SQP & monitor	SIP/SQP Delivery is the responsibility of the SIP Program Manager and follows Change Management and project management processes. While Service Level Management is a	Service Level Manager

Process ID	Procedure or Decision	Description	Role
		key stakeholder in the SIP/SQP process, the team is not responsible for actual delivery. The SIP/SQP Program Board is responsible for monitoring the progress of the SIP/SQP through regular progress reports. Service Level Management monitors all ongoing SIPs/SQPs ensuring they remain focused on business objectives and to provide input to Service Review meetings. Go to SD 2.8.6 to review the SIP/SQP.	
SD 2.8.6	Review SIP/SQP	Change Management feeds into this activity advising that the Change record has been closed. When the SIP/SQP is nearing completion, the SIP/SQP Program Board assesses the likely success against the CSFs and accompanying KPIs. A short evaluation report is produced which provides recommendations for closure or further actions Go to SD 2.8.7 to determine whether to close the SIP/SQP.	Service Level Manager
SD 2.8.7	Close SIP/SQP?	If yes, go to SD 2.8.8 to monitor SIP/SQP requirements. If no, go to SD 2.8.1 to identify Service improvement requirements.	Service Level Manager
SD 2.8.8	Close & Monitor SIP/SQP	Once the SIP/SQP is closed, monitor for a period of time to allow the benefits of the project to take effect. The SIP/SQP Program Board retains responsibility for the monitoring period and will determine when it can end. The Service Improvement Program process ends.	Service Level Manager

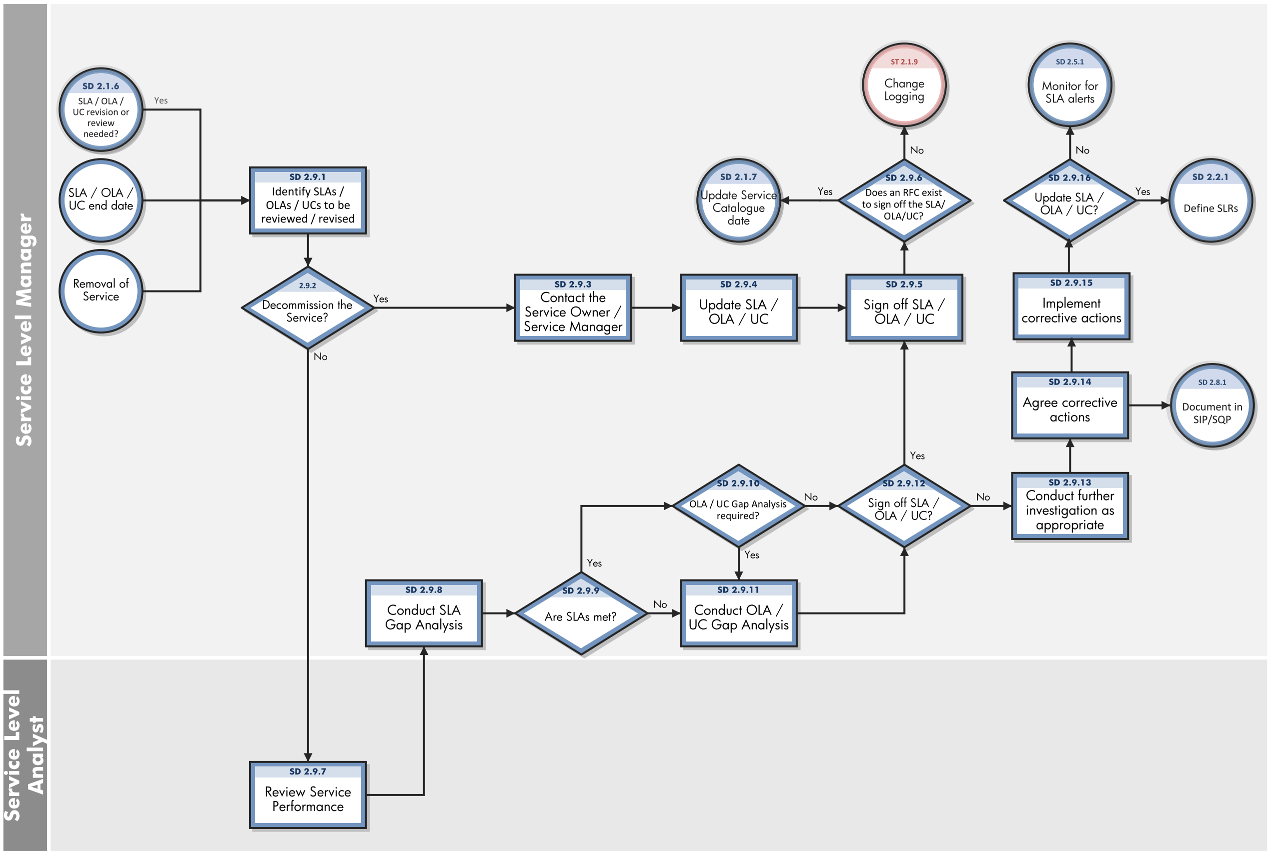


Review and Revise SLAs/OLAs/UCs (SD 2.9)

Process ID	Procedure or Decision	Description	Role
SD 2.9.1	Identify SLAs /OLAs/UCs to be reviewed / revised	Conduct an investigation of SLAs /OLAs/UCs to identify all agreements that require review. Go to SD 2.9.2 to determine whether to decommission the Service.	Service Level Manager
SD 2.9.2	Decommission the Service?	If yes, go to SD 2.9.3 to contact the Service Owner or Service Manager. If no, go to SD 2.9.7 to review the Service performance.	Service Level Manager
SD 2.9.3	Contact the Service Owner / Service	The Service Level Manager works with the Service Owners and Service Managers to review the SLAs/OLAs/UCs. Go to SD 2.9.4 to update the SLA /OLA/UC.	Service Level Manager

Process ID	Procedure or Decision	Description	Role
	Manager		
SD 2.9.4	Update SLA /OLA/UC	The Service Level Manager updates the SLA with the Customer to reflect the decommissioning of the Service. The Service Level Manager updates the OLA/UC with the Service Owner and Supplier Manager to reflect the decommissioning of the Service. Go to SD 2.9.5 to sign-off the SLA /OLA/UC.	Service Level Manager
SD 2.9.5	Sign off SLA /OLA/UC	The SLAs /OLAs/UCs are signed off following the review. Go to SD 2.9.6 to determine whether an RFC exists.	Service Level Manager
SD 2.9.6	Does an RFC exist to sign off the SLA /OLA/UC?	If yes, go to Maintain the Service Catalog (SD 2.1.7) to update the Service Catalog. If no, go to Change Logging (ST 2.1.9) to create a new Change.	Service Level Manager
SD 2.9.7	Review Service performance	Obtain data from other Service management processes to assess the performance of actual results against agreed targets. Go to SD 2.9.8 to conduct an SLA gap analysis.	Service Level Analyst
SD 2.9.8	Conduct SLA Gap Analysis	Prepare an SLA Gap Analysis to identify the shortfalls in SLA results against the business requirements and document in a report. Shortfalls will need to be addressed within a SIP. Go to SD 2.9.9 to determine whether the agreed SLAs are being met.	Service Level Manager
SD 2.9.9	Are SLAs met?	If yes, go to SD 2.9.10 to determine whether an OLA/UC Gap Analysis is required. If no, go to SD 2.9.11 to conduct an OLA/UC Gap Analysis.	Service Level Manager
SD 2.9.10	OLA/UC Gap Analysis required?	If yes, go to SD 2.9.11 to conduct an OLA/UC Gap Analysis. If no, go to SD 2.9.12 to determine whether to sign-off the SLA /OLA/UC.	Service Level Manager
SD 2.9.11	Conduct OLA/UC Gap Analysis	Review the Service delivery chain and identify all OLAs/UCs which support delivery of the Service. Conduct an appropriate Gap Analysis to identify shortfalls against agreed targets and document. Go to SD 2.9.12 to determine whether to sign-off the SLA /OLA/UC.	Service Level Manager

Process ID	Procedure or Decision	Description	Role
SD 2.9.12	Sign off SLA /OLA/UC?	If yes, go to SD 2.9.5 to sign-off the SLA /OLA/UC. If no, go to SD 2.9.13 to conduct further investigation as appropriate.	Service Level Manager
SD 2.9.13	Conduct further investigation as appropriate	Conduct further investigation to ensure issues are removed and the SLA / OLA / UC can be signed off. Go to SD 2.9.14 to agree corrective actions-	Service Level Manager
SD 2.9.14	Agree corrective actions	Identify and agree corrective actions with the Service Owner and Supplier Manager and document them in the SIP/SQP. Go to SD 2.9.15 to implement corrective actions.	Service Level Manager
SD 2.9.15	Implement corrective actions	Implement corrective actions. Go to SD 2.9.16 to determine whether to update the SLA/OLA/UC.	Service Level Manager
SD 2.9.16	Update SLA/OLA/ UC?	If yes, go to Create or Amend Services (SD 2.2.1) to define requirements. If no, go to Monitor Service Levels (SD 2.5.1) to monitor for SLA alerts.	Service Level Manager


Service Level Manager
Service Level Analyst
SD 2.1.6
SLA / OLA / UC revision or review needed?
Yes
SLA / OLA / UC end date
Removal of Service
SD 2.9.1
Identify SLAs / OLAs / UCs to be reviewed / revised
2.9.2
Decommission the Service?
Yes
No
SD 2.9.3
Contact the Service Owner / Service Manager
SD 2.9.4
Update SLA / OLA / UC
SD 2.9.5
Sign off SLA / OLA / UC
SD 2.1.7
Update Service Catalogue date
Yes
SD 2.9.6
Does an RFC exist to sign off the SLA/ OLA/UC?
No
ST 2.1.9
Change Logging
SD 2.5.1
Monitor for SLA alerts
No
SD 2.9.16
Update SLA / OLA / UC?
Yes
SD 2.2.1
Define SLRs
SD 2.9.15
Implement corrective actions
SD 2.9.14
Agree corrective actions
SD 2.8.1
Document in SIP/SQP
Yes
SD 2.9.10
OLA / UC Gap Analysis required?
No
SD 2.9.12
Sign off SLA / OLA / UC?
No
SD 2.9.13
Conduct further investigation as appropriate
Yes
Yes
SD 2.9.8
Conduct SLA Gap Analysis
SD 2.9.9
Are SLAs met?
No
SD 2.9.11
Conduct OLA / UC Gap Analysis
SD 2.9.7
Review Service Performance

Chapter 24: Service Level Management Details

HP Service Manager uses the Service Level Management module to enable the Service Level Management process. The main function of Service Level Management is to improve the quality of services that you provide to customers. Service Level Managers, Supplier Managers and customers work together to ensure the various agreements are correctly documented and monitored.

This section describes selected Service Level Management details in the out-of-box Service Manager system.

- An SLA is:

  A service-level agreement (SLA) is an agreement between two or more parties, where one is the customer (business) and the others are service providers. This can be a legally binding formal or an informal "contract".

  Service level agreements are also defined at different levels:

  - Customer-based SLA:

    An agreement with an individual customer group, covering all the services they use.

  - Service-based SLA:

    An agreement for all customers using the services being delivered by the service provider.

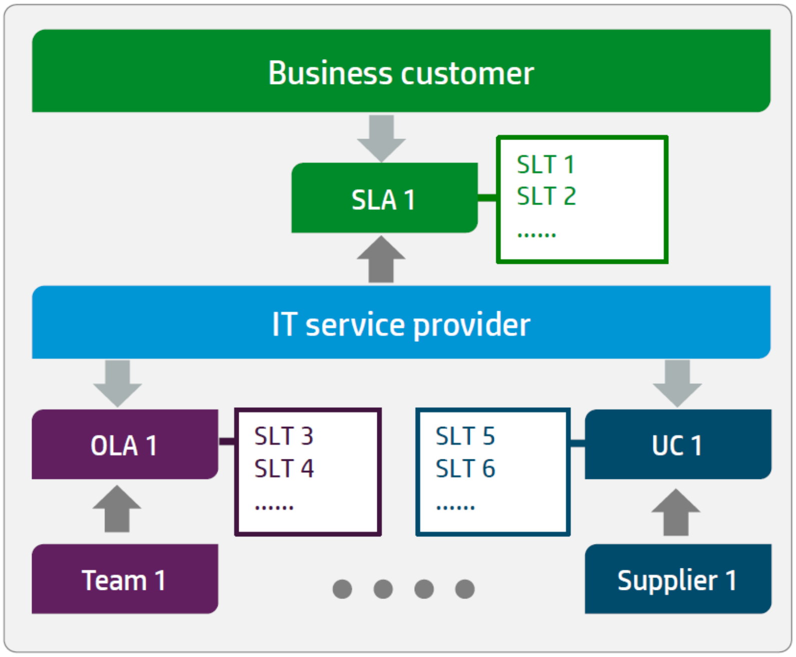
- An OLA is:

  An operational-level agreement (OLA) defines the interdependent relationships among the internal support groups of an IT organization working to support a service-level agreement (SLA). The agreement describes the responsibilities of each internal support group toward other support groups, including the process and timeframe for delivery of their services. The objective of the OLA is to present a clear, concise and measurable description of the service provider's internal support relationships.

- A UC is:

  An Underpinning Contract (UC) is a legally binding contract between IT service provider and supplier or third party to deliver agreed level of service quality or goods at specified time.

The relation between these three elements is defined in the graphic below.



Topics in this section include:

"The Workflow for Agreements, Underpinning Contracts" below

"Creating a new SLA, OLA or UC" on page 374

"The Draft phase" on page 375

"The Review phase" on page 375

"The Agreed phase" on page 376

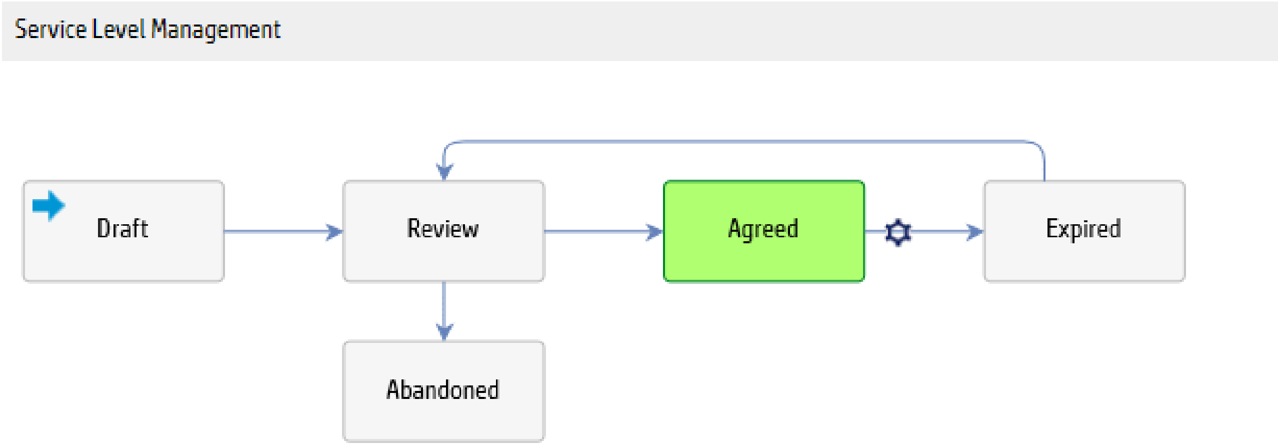
"The Expired phase" on page 378

"Service Reviews and usages of SIPs/SQPs" on page 378

"Service Level Management form details" on page 383

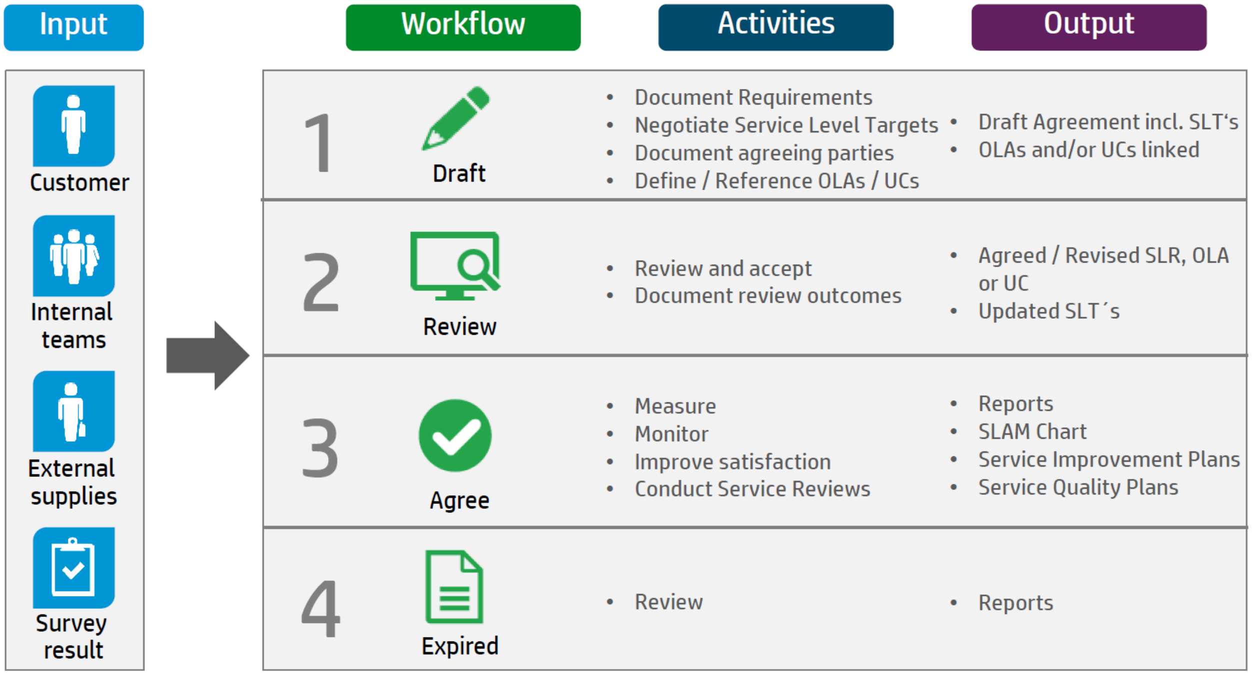
The Workflow for Agreements, Underpinning Contracts

The full Service Level Management module was moved towards Process Designer. As part of this step, the following workflow was introduced to support the several activities in the Service Level Management process.



Phase	Description
Draft	Initialize a new SLR, OLA or UC in draft phase to document all required details
Review	Review with the various stakeholders the documented details prior activating the SLA, OLA or UC
Agreed	The SLA, OLA and UC are agreed and active.
Expired	The SLA, OLA and UC are expired and inactive.
Abandoned	The SLA, OLA and UC have been abandoned.

The different activities in the workflow phases are summarized as follow.



Input

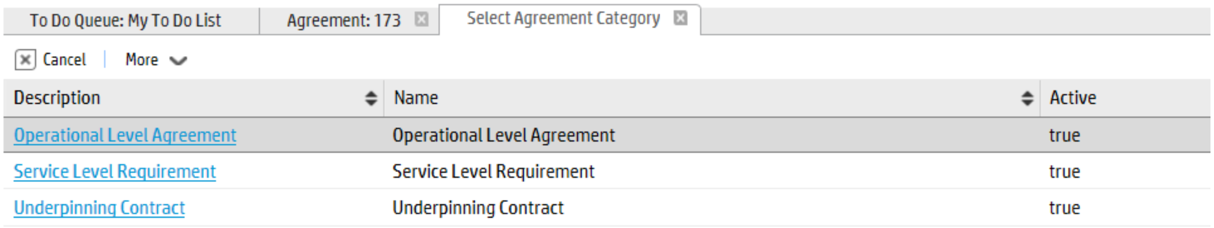
- Customer
- Internal teams
- External supplies
- Survey result

	Workflow	Activities	Output
1	Draft	Document Requirements Negotiate Service Level Targets Document agreeing parties Define / Reference OLAs / UCs	Draft Agreement incl. SLT‘s OLAs and/or UCs linked
2	Review	Review and accept Document review outcomes	Agreed / Revised SLR, OLA or UC Updated SLT´s
3	Agree	Measure Monitor Improve satisfaction Conduct Service Reviews	Reports SLAM Chart Service Improvement Plans Service Quality Plans
4	Expired	Review	Reports

Creating a new SLA, OLA or UC

To create a new SLA, OLA or UC, click **Service Level Management** > **Agreements** > **New Agreement**, and then select the agreement category.

- To start a new SLA, select **Service Level Requirement**, since every SLA starts with documented SLRs. Once an SLR is agreed it becomes an SLA.
- To create a new OLA or UC, select the correct category.

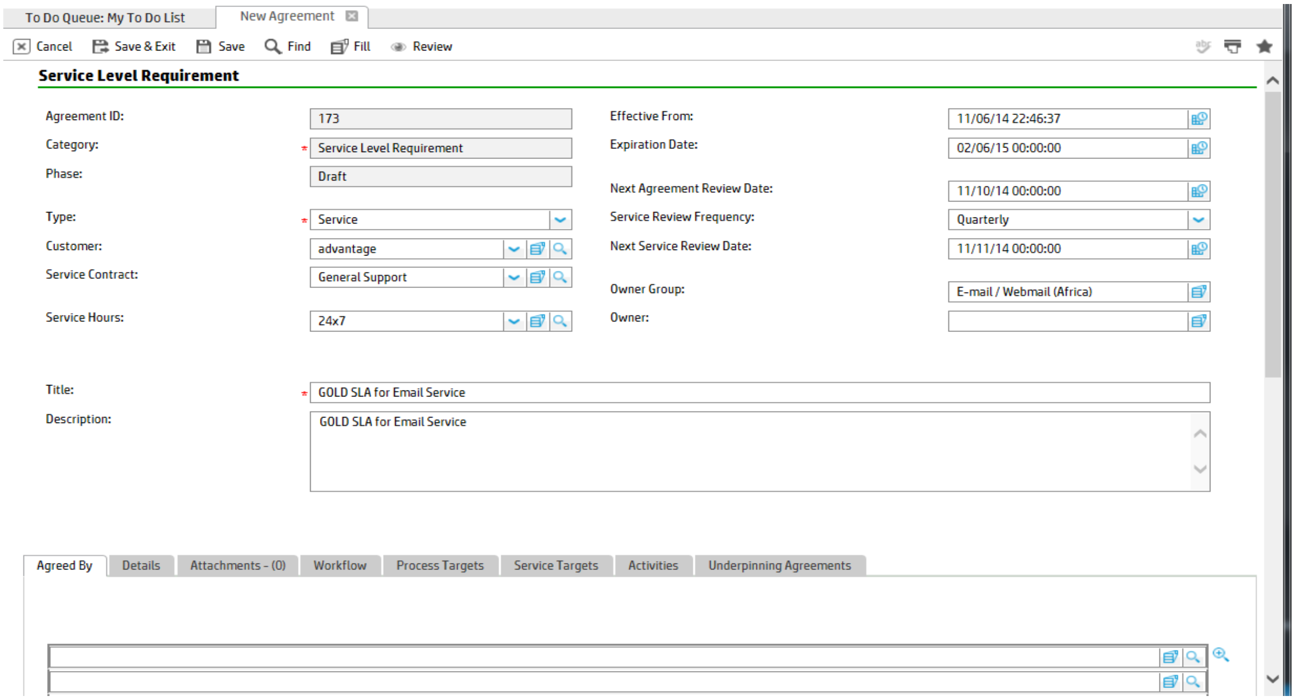


Description	Name	Active
Operational Level Agreement	Operational Level Agreement	true
Service Level Requirement	Service Level Requirement	true
Underpinning Contract	Underpinning Contract	true

The Draft phase

Every record type in Service Level Management module starts from draft phase. In draft phase, you can document some general requirements and the requested Service Level Targets. Process Targets represent response targets, whereas Service Targets measure the availability.

Ensure that you document all required fields. Click the **Review** button to move the record into the next phase.



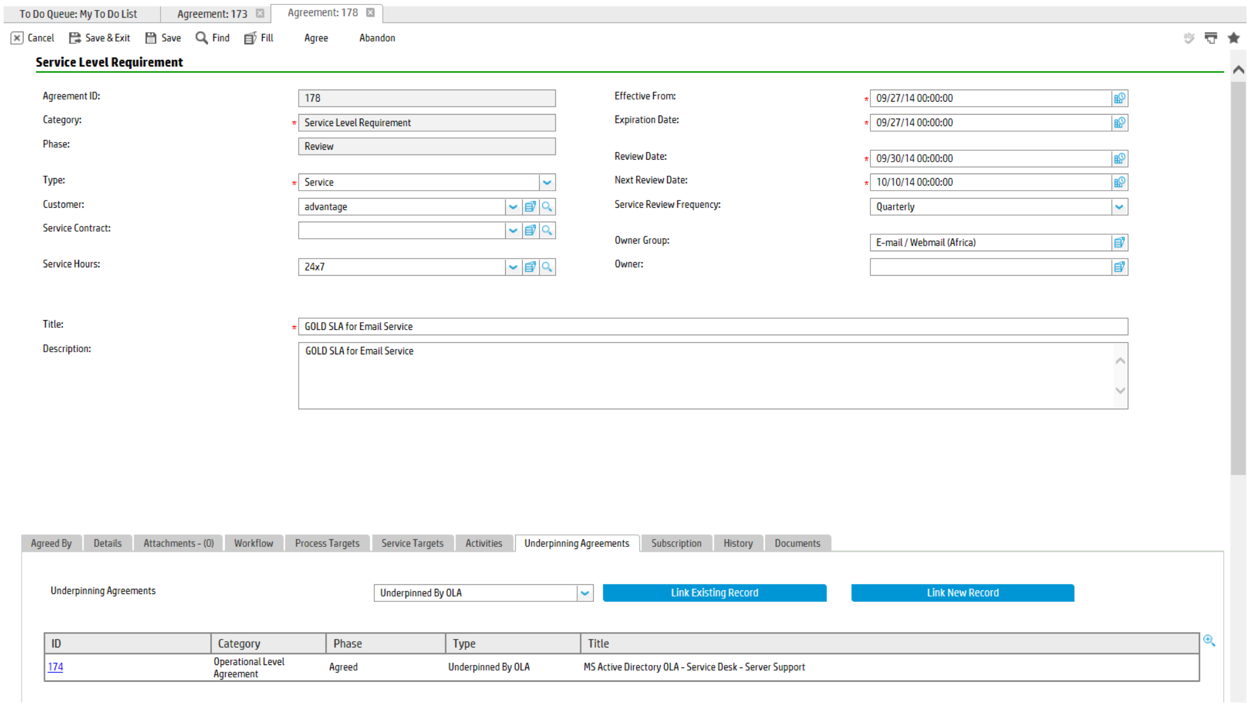
Service Level Requirement

Agreement ID:	173	Effective From:	11/06/14 22:46:37
Category:	* Service Level Requirement	Expiration Date:	02/06/15 00:00:00
Phase:	Draft	Next Agreement Review Date:	11/10/14 00:00:00
Type:	* Service	Service Review Frequency:	Quarterly
Customer:	advantage	Next Service Review Date:	11/11/14 00:00:00
Service Contract:	General Support	Owner Group:	E-mail / Webmail (Africa)
Service Hours:	24x7	Owner:	
Title:	* GOLD SLA for Email Service		
Description:	GOLD SLA for Email Service		

The Review phase

In Review phase, all stakeholders have the chance to review the agreed details and adjust in case requirements have changed or cannot be met. The review phase is the last prior to activating the agreement or contract.

The review phase should be used to double-check whether all underpinning OLAs and contracts meet the agreed targets of the SLA. By looking at the **Underpinning Agreement** tab the Service Level Manager can easily verify the associated OLAs/UCs.



Service Level Requirement

Agreement ID:	178	Effective From:	09/27/14 00:00:00
Category:	Service Level Requirement	Expiration Date:	09/27/14 00:00:00
Phase:	Review	Review Date:	09/30/14 00:00:00
Type:	Service	Next Review Date:	10/10/14 00:00:00
Customer:	advantage	Service Review Frequency:	Quarterly
Service Contract:		Owner Group:	E-mail / Webmail (Africa)
Service Hours:	24x7	Owner:	

Title: GOLD SLA for Email Service

Description: GOLD SLA for Email Service

Underpinning Agreements: Underpinned By OLA

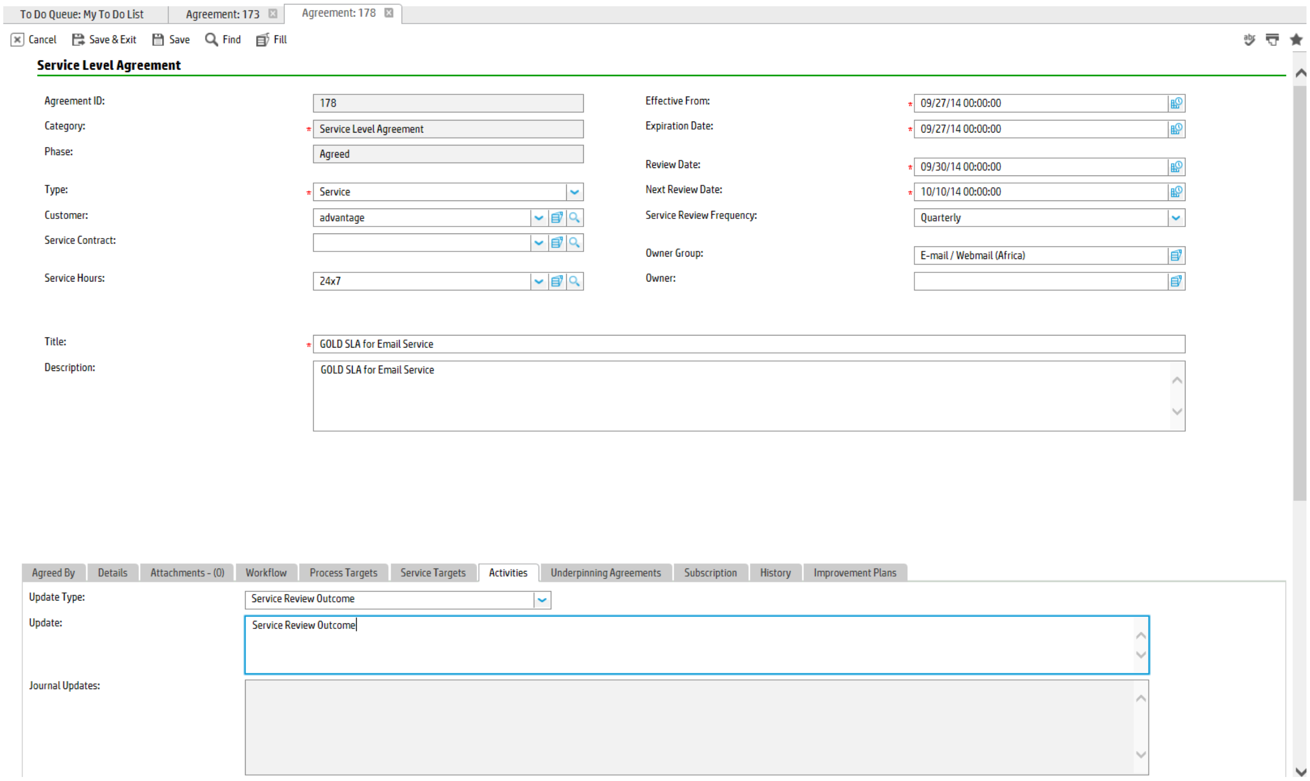
ID	Category	Phase	Type	Title
174	Operational Level Agreement	Agreed	Underpinned By OLA	MS Active Directory OLA - Service Desk - Server Support

In accordance to ITIL guidance, all OLAs/UCs should support the defined SLAs within the business. Where specific clauses and targets are required for an individual service, the conditions in the SLTs of the OLA/UC should be leveraged. By using the conditioned SLTs of the OLA/UC, the Service Level Manager can ensure that the agreed targets of the SLA are correctly covered.

The Agreed phase

In the Agreed phase, the SLM records are active and used. In case modifications are required, the SLA, OLA,or UC is directly updated in this phase. Service Reviews help to keep the records up to date. All changes have to go through Change Management and shall be tracked in the activity log.

The system allows to document SIPs and SQP directly from the agreement. This helps to validate the actions directly in each service review. To document service reviews activities, you can use the activity log.



Service Level Agreement

Agreement ID:	178	Effective From:	09/27/14 00:00:00
Category:	Service Level Agreement	Expiration Date:	09/27/14 00:00:00
Phase:	Agreed	Review Date:	09/30/14 00:00:00
Type:	Service	Next Review Date:	10/10/14 00:00:00
Customer:	advantage	Service Review Frequency:	Quarterly
Service Contract:		Owner Group:	E-mail / Webmail (Africa)
Service Hours:	24x7	Owner:	

Title: GOLD SLA for Email Service

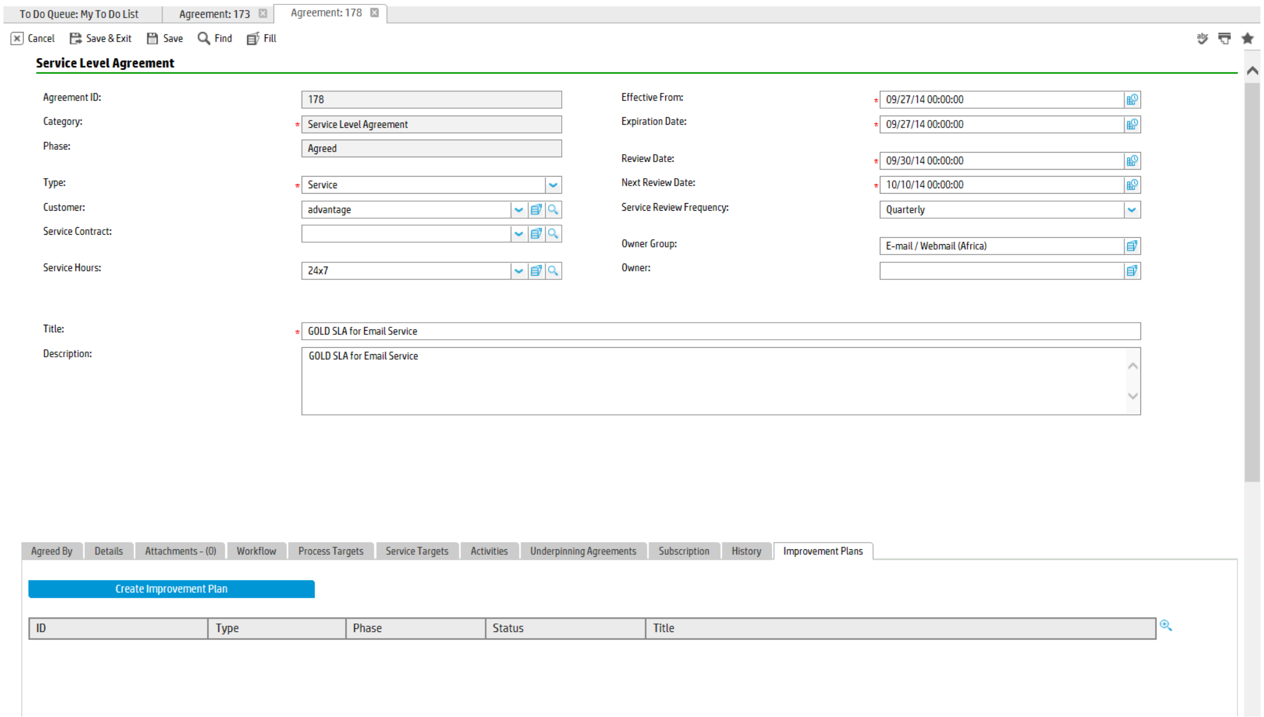
Description: GOLD SLA for Email Service

Update Type: Service Review Outcome

Update: Service Review Outcome

Journal Updates:

To document SIP/ SQP, you can use the Improvement Plan feature.



Service Level Agreement

Agreement ID:	178	Effective From:	09/27/14 00:00:00
Category:	Service Level Agreement	Expiration Date:	09/27/14 00:00:00
Phase:	Agreed	Review Date:	09/30/14 00:00:00
Type:	Service	Next Review Date:	10/10/14 00:00:00
Customer:	advantage	Service Review Frequency:	Quarterly
Service Contract:		Owner Group:	E-mail / Webmail (Africa)
Service Hours:	24x7	Owner:	

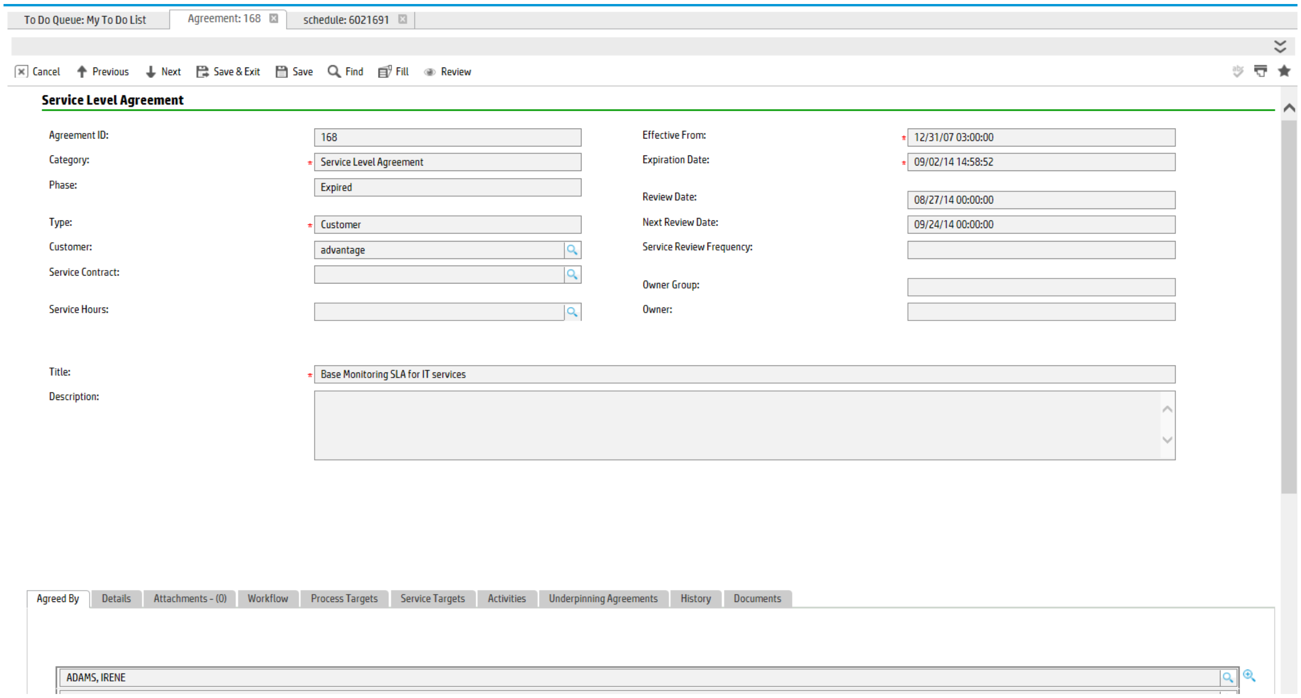
Title: GOLD SLA for Email Service

Description: GOLD SLA for Email Service

ID	Type	Phase	Status	Title

The Expired phase

The system automatically moves the record into the expired phase once the expiration date has been reached. In expired phase, the records are inactive and read-only. In case the record needs to be re-activate, click the **Review** button to move it back to Review phase.



Service Level Agreement

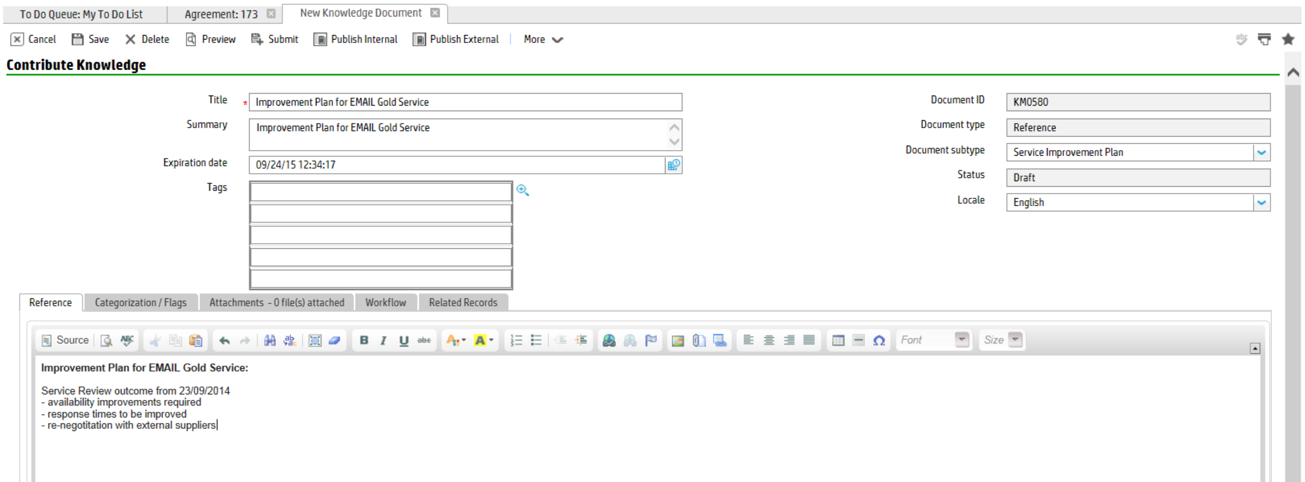
Agreement ID:	168	Effective From:	12/31/07 03:00:00
Category:	Service Level Agreement	Expiration Date:	09/02/14 14:58:52
Phase:	Expired	Review Date:	08/27/14 00:00:00
Type:	Customer	Next Review Date:	09/24/14 00:00:00
Customer:	advantage	Service Review Frequency:	
Service Contract:		Owner Group:	
Service Hours:		Owner:	
Title:	Base Monitoring SLA for IT services		
Description:			

ADAMS, IRENE

Service Reviews and usages of SIPs/SQPs

Service Reviews meetings should be conducted frequently. The outcome of these meetings are documented in either Service Improvement or Service Quality Plans. Service Manager allows to document the details of the service reviews by leveraging the knowledge management module.

To create an SIP or SQP, click the **Create Improvement Plan** button.



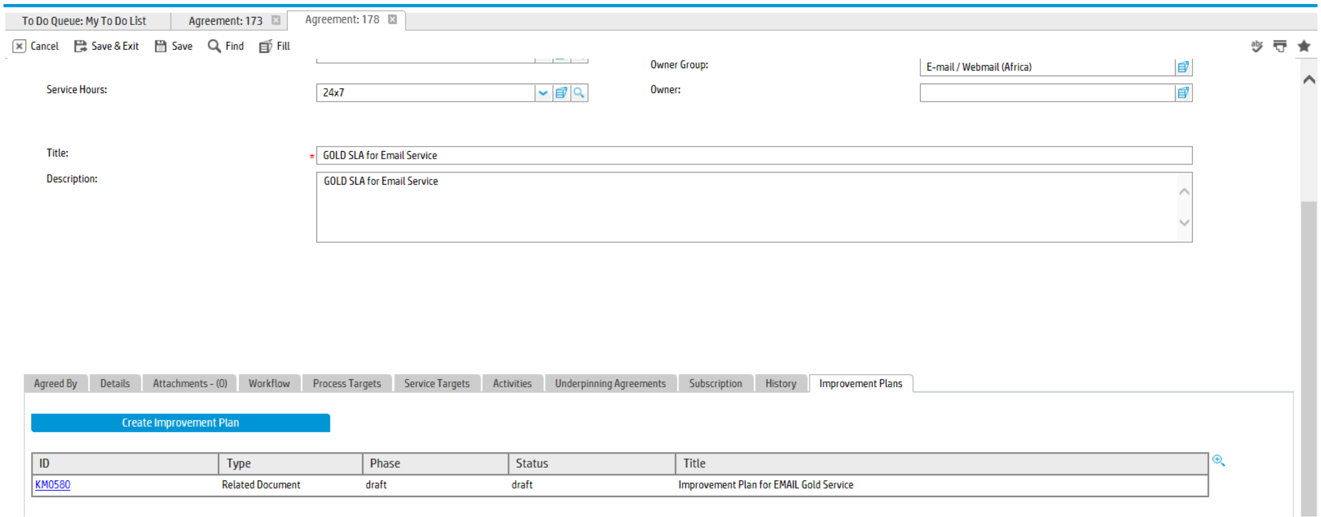
Contribute Knowledge

Title	Improvement Plan for EMAIL Gold Service	Document ID	KM0580
Summary	Improvement Plan for EMAIL Gold Service	Document type	Reference
Expiration date	09/24/15 12:34:17	Document subtype	Service Improvement Plan
Tags		Status	Draft
		Locale	English

Improvement Plan for EMAIL Gold Service:

Service Review outcome from 23/09/2014
- availability improvements required
- response times to be improved
- re-negotiation with external suppliers

All SIPs/SQPs are listed directly in the Service Level Management record.



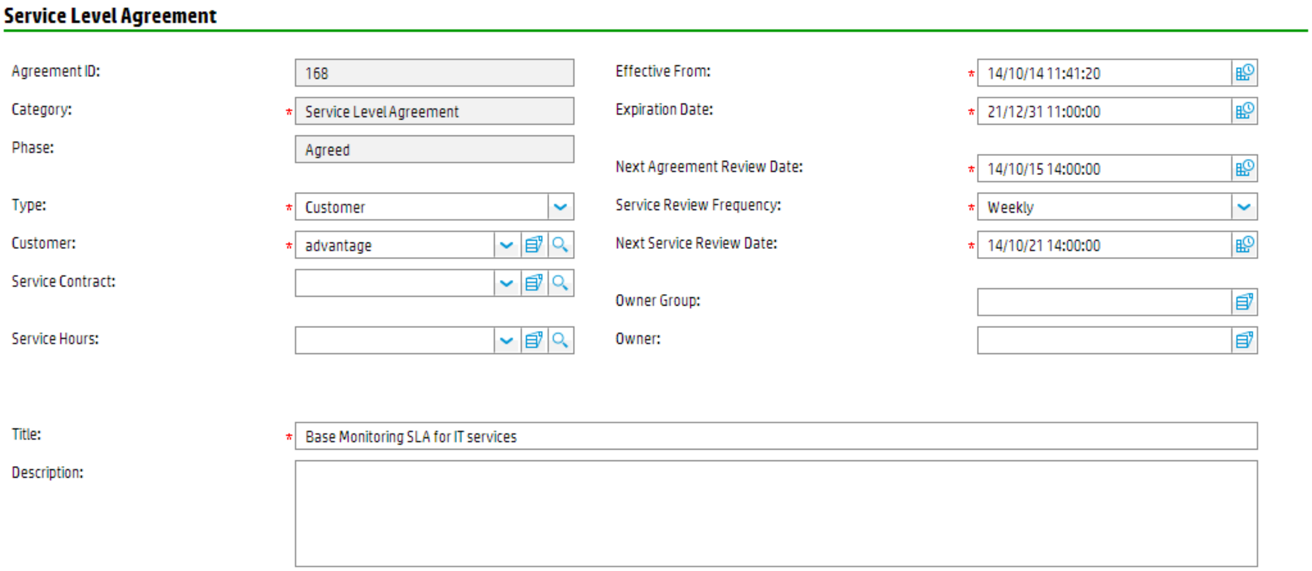
		Owner Group:	E-mail / Webmail (Africa)
Service Hours:	24x7	Owner:	
Title:	GOLD SLA for Email Service		
Description:	GOLD SLA for Email Service		

ID	Type	Phase	Status	Title
KM0580	Related Document	draft	draft	Improvement Plan for EMAIL Gold Service

Service Level Management forms

The following forms are Service Level Management forms.

Service Level Agreement



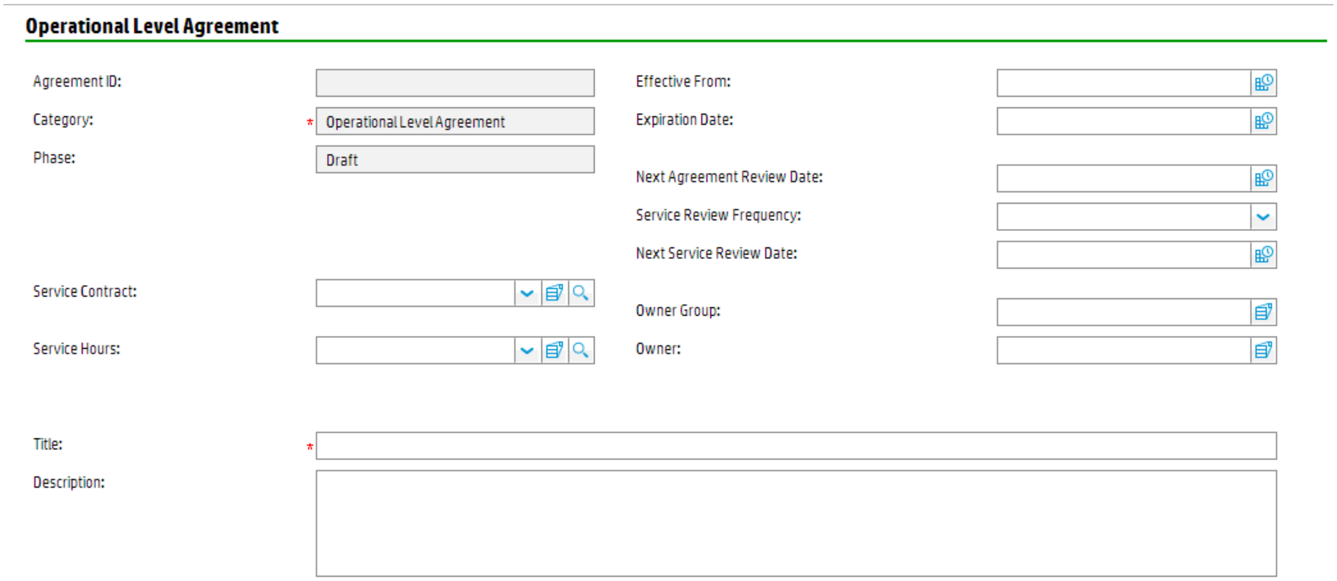
Service Level Agreement

Agreement ID:	168	Effective From:	* 14/10/14 11:41:20
Category:	* Service Level Agreement	Expiration Date:	* 21/12/31 11:00:00
Phase:	Agreed	Next Agreement Review Date:	* 14/10/15 14:00:00
Type:	* Customer	Service Review Frequency:	* Weekly
Customer:	* advantage	Next Service Review Date:	* 14/10/21 14:00:00
Service Contract:		Owner Group:	
Service Hours:		Owner:	

Title: * Base Monitoring SLA for IT services

Description:

Operational Level Agreement



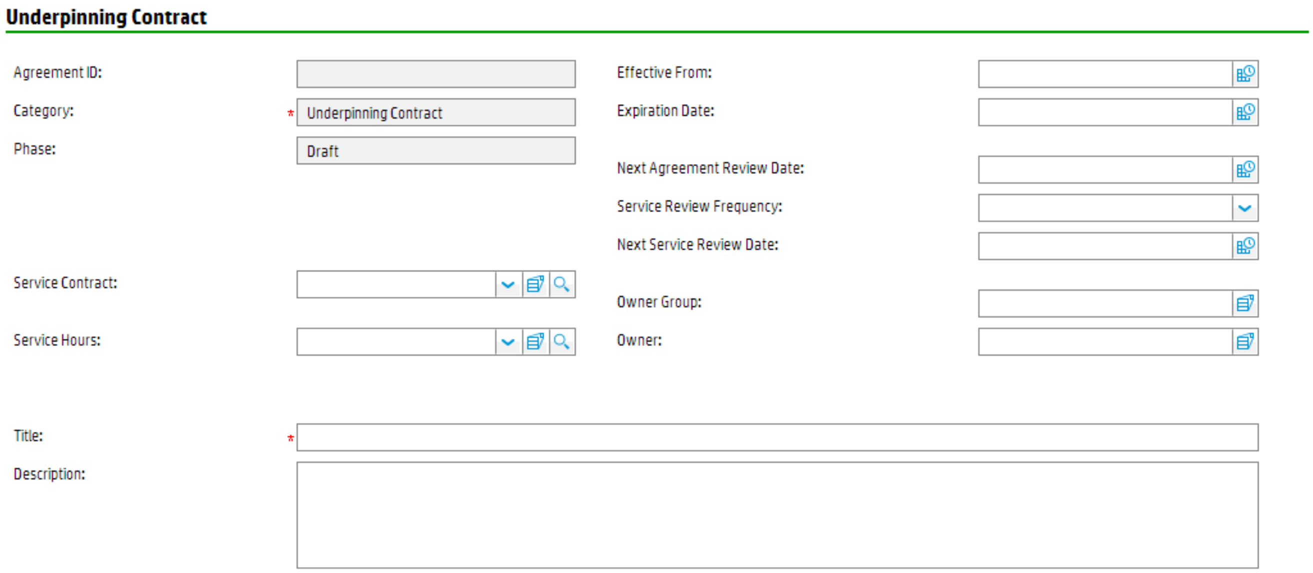
Operational Level Agreement

Agreement ID:		Effective From:	
Category:	* Operational Level Agreement	Expiration Date:	
Phase:	Draft	Next Agreement Review Date:	
		Service Review Frequency:	
		Next Service Review Date:	
Service Contract:		Owner Group:	
Service Hours:		Owner:	

Title: *

Description:

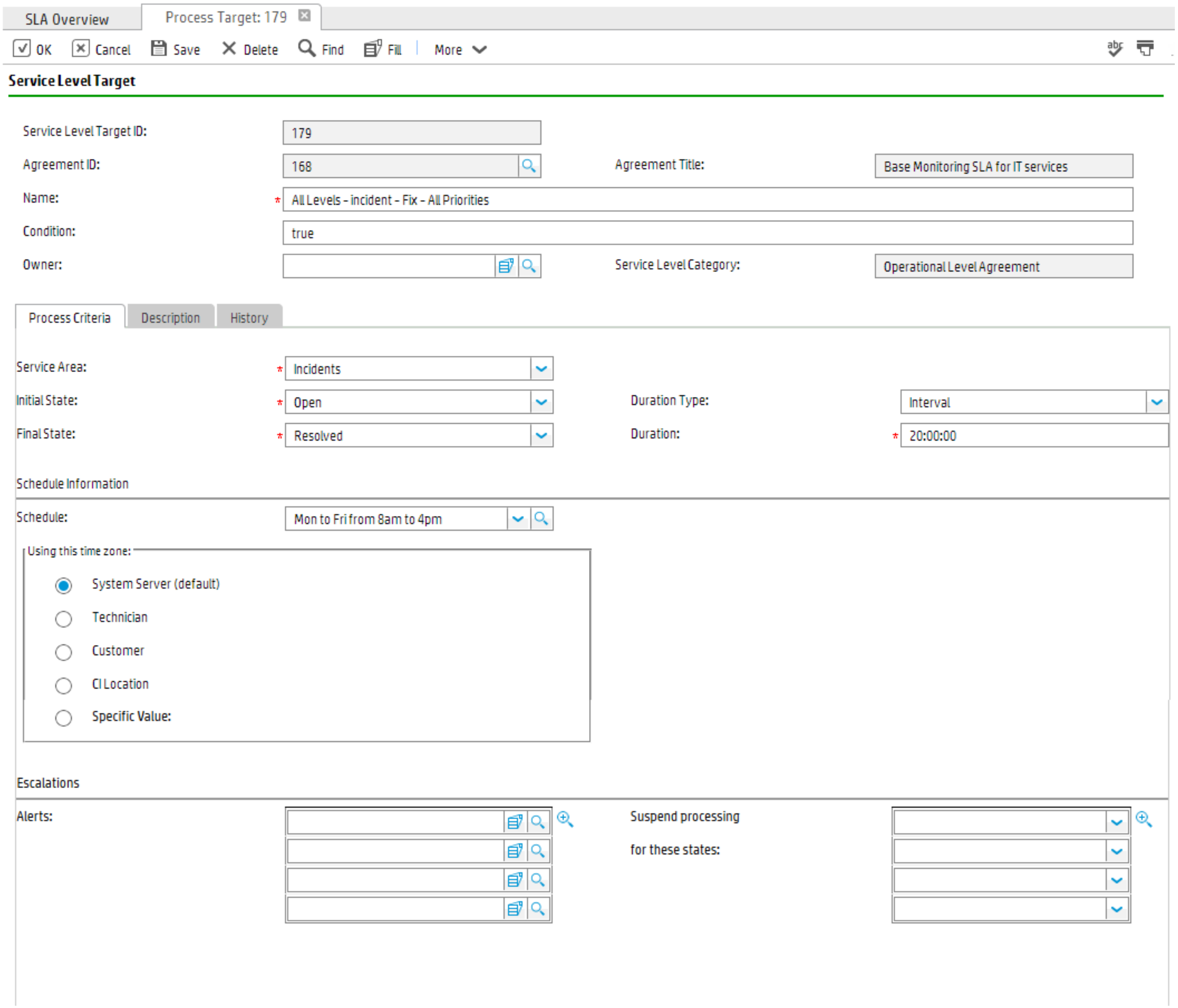
Underpinning Contract



Underpinning Contract

Agreement ID:		Effective From:	
Category:	* Underpinning Contract	Expiration Date:	
Phase:	Draft		
		Next Agreement Review Date:	
		Service Review Frequency:	
		Next Service Review Date:	
Service Contract:		Owner Group:	
Service Hours:		Owner:	
Title:	*		
Description:			

Service Level Target - Process Target



Service Level Target

Service Level Target ID:	179		
Agreement ID:	168	Agreement Title:	Base Monitoring SLA for IT services
Name:	* All Levels - incident - Fix - All Priorities		
Condition:	true		
Owner:		Service Level Category:	Operational Level Agreement

Service Area:	* Incidents		
Initial State:	* Open	Duration Type:	Interval
Final State:	* Resolved	Duration:	* 20:00:00

Schedule Information

Schedule: Mon to Fri from 8am to 4pm

Using this time zone:

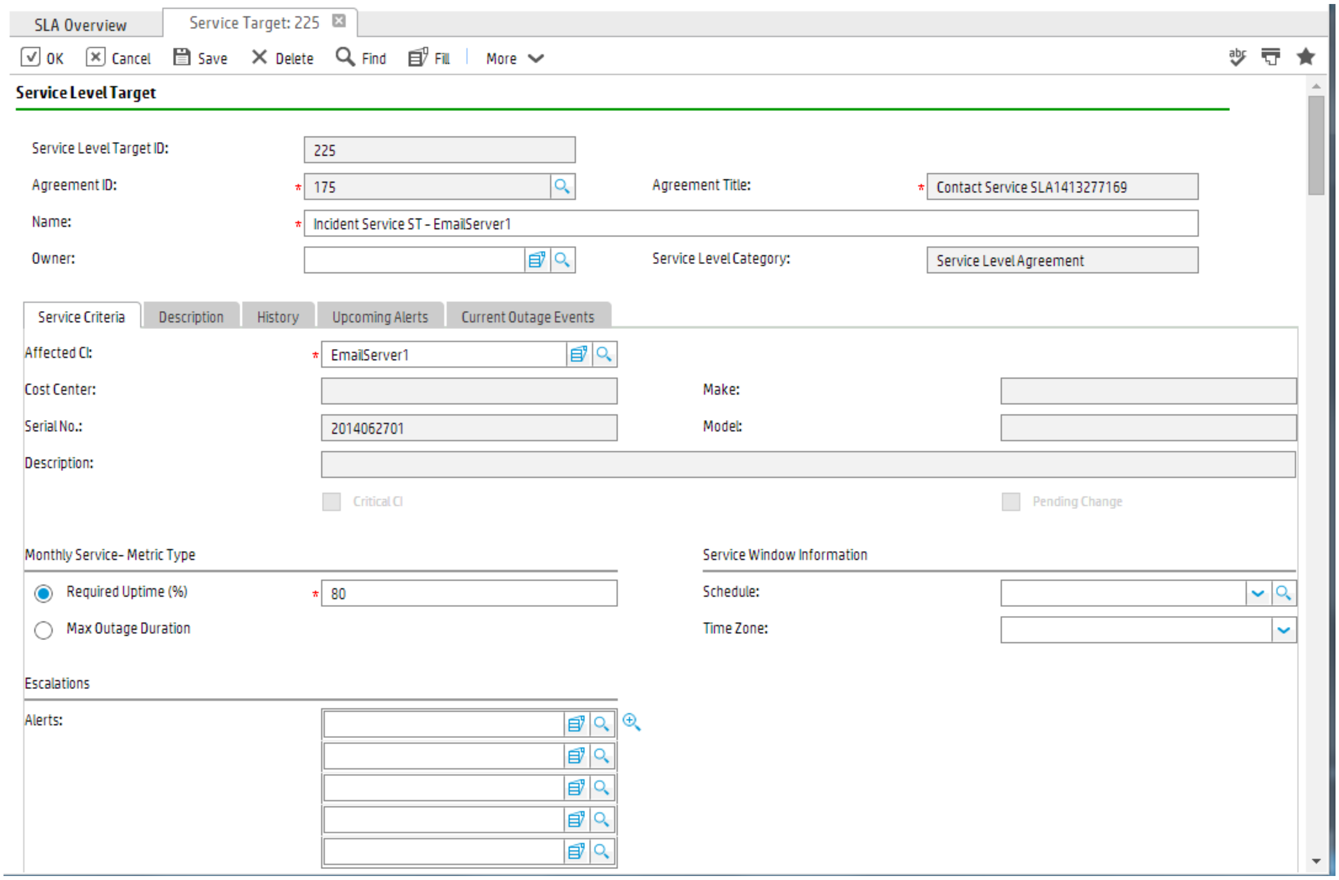
● System Server (default)
○ Technician
○ Customer
○ CI Location
○ Specific Value:

Escalations

Alerts:

Suspend processing for these states:

Service Level Target - Service Target



Service Level Target

Service Level Target ID: 225

Agreement ID: * 175

Agreement Title: * Contact Service SLA1413277169

Name: * Incident Service ST - EmailServer1

Owner:

Service Level Category: Service Level Agreement

Service Criteria | Description | History | Upcoming Alerts | Current Outage Events

Affected CI: * EmailServer1

Cost Center:

Make:

Serial No.: 2014062701

Model:

Description:

□ Critical CI

□ Pending Change

Monthly Service- Metric Type

● Required Uptime (%) * 80

○ Max Outage Duration

Service Window Information

Schedule:

Time Zone:

Escalations

Alerts:

Service Level Management form details

The following table identifies and describes some of the features of Service Level Management forms.

SLA/OLA/UC field descriptions

Label	Description
MAIN	
Agreement ID	The unique ID of the Agreement. HP Service Manager populates this field when the Agreement is first created. Service Manager uses this number to track relationships between Agreements and their supporting data.
Category	The category of agreement that best describes the Agreement.
Phase	The current phase of the record.
Type	The type field identifies an Agreement as a Service or

Label	**Description**
	Customer Agreement. This field has two possible values: Service or Customer.
Customer	The name of the customer who is directly impacted by the service levels measured by the Agreement.
Service Contract	The ID of the contract (entitlement) that covers the service specified in the Agreement. The contracts available in the drop-down list are dependent on the selected customer for the Agreement.
Service Hours	The schedule that customers are entitled to the service guaranteed by the Service Level Agreement (SLA). When you register Interactions or open Incidents, HP Service Manager checks the Service Hours schedule, to determine if the customer submitting the Interaction or Incident is entitled to the service.
Title	A brief descriptive title for the Agreement.
Description	A description of the service levels covered by the Agreement.
Effective From	The date and time when the Agreement coverage begins.
Expiration Date	The date and time when the Agreement coverage expires.
Next Agreement Review Date	The date when the agreement is supposed to be reviewed next time.
Service Review Frequency	This field identifies how often the agreement is to be reviewed.
Next Service Review Date	The date when the relevant service in the agreement is supposed to be reviewed next time.
Owner Group	The group who is responsible for the agreement.
Owner	The operator who is responsible for the agreement.
Agreed By	
The individuals in the contacts table who reach an agreement on the Agreement.	
Details	
Notes, verbal agreements, or comments that are relevant to the Agreement. For example, an additional agreement that was not part of the original agreement.	
Attachments	

Label	Description
You can use the Attachments section to attach documents to the Agreement.	
Workflow	
Displays a figure of request task workflow. It indicates the current phase which the request task is in, and traces the phase transition history.	
Process Targets	
Displays the Service Level Targets which define the Process Target details.	
Service Targets	
Displays the Service Level Targets which define the Service Target details.	
Activities	
Records information that the operator enters during the lifecycle of the Agreement. Every time you update the agreement, you can fill in an update on the Activities section. A log of all the updates is stored on the Journal Updates and activities list.	
Underpinning Agreements	
Displays a list of Underpinning Agreements related to this Agreement.	
Subscriptions	
Displays a list of subscription information related to this Agreement.	
History	
Displays the monthly overall performance metrics of this Agreement, as well as the specific performance metrics of its different types of service level targets (process targets and service targets).	
Improvement Plans	
Displays a list of Improvement Plans related to this Agreement.	
Assignment Groups	
The group in the assignment table associated with agreement for Operational Level Agreement.	
Related SLA	
Displays a list of SLAs related to this Operational Level Agreement.	
External Assignment Groups	
The external group in the assignment table associated with agreement for Underpinning Contract.	

Service Level Target field descriptions

Label	Description
MAIN	
Service Level Target ID	The unique ID of the Process or Service Target. HP Service Manager creates this field automatically when adding the SLT. This field is read-only unless you are searching for specific SLTs.
Agreement ID	The unique ID of the Agreement associated to the Service Target. HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard. Service Manager uses this number to track relationships between Agreements and their supporting data.
Name	The name of the Process or Service Target.
Condition	Determines whether to process the process Target. You can enter the condition manually, or HP Service Manager can create it automatically based on field parameters that you select when you add the SLT by using the wizard.
Owner	The owner of the process for the Process or Service Target.
Agreement Title	The title of the Agreement associated to the Service Target.
Service Level Category	The service level category of agreement that best describes the Service Target.
Process Criteria	
Service Area	The application area in HP Service Manager that the Process Target applies to. The value displayed in the drop-down list reflect the HP Service Manager areas or modules that are available for use in Service Level Agreement.
Initial State	A state when the Process Target (SLT) should start measuring the process time.
Final State	A state when the Process Target (SLT) should stop measuring the process time.
Duration Type	The type of response time to measure when processing the Process Target.
Duration	The maximum interval of time allowed between the Initial State and the Final State.
Schedule Information - Schedule	The schedule used to determine the valid times for processing the Process Target.
Schedule Information - Using this time	The time zone to use when processing the Process Target.

Label	Description
zone	
Escalation - Alerts	The alert(s) to generate when processing the Process Target.
Escalation - Suspend processing for these states	States when processing for the Service Level Target (SLT) should be suspended.
Description	
Displays a list of subscription information related to this Service Level Target.	
History	
Displays the timestamps and operators that the Service Level Target is opened or updated by.	
Service Criteria	
Affected CI	The unique ID of the affected configuration item (CI) measured by the Service Target. The CI is required to have a valid identifier and must have a corresponding entry in the device table.
Cost Center:	The cost center information for this configuration item (CI). HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard.
Serial No.	The serial number for this configuration item (CI). HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard.
Description	The manufacturer's model identification for this configuration item (CI). HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard.
Make	The manufacturer of this configuration item (CI). HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard.
Model	The manufacturer's model identification for this configuration item (CI). HP Service Manager populates this field when you create a new SLT from the Agreement screen using the wizard.
Monthly Service-Metric Type - Required Uptime	The percentage of time that the affected configuration item (CI) should be available per month.
Monthly Service-Metric Type - Max Outage Duration	The maximum amount of time that the affected configuration item (CI) may be unavailable for a single outage.

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Service Window Information - Schedule</td><td>The schedule used to determine the valid times for processing the Service Target.</td></tr>
<tr><td>Service Window Information - Time Zone</td><td>The time zone to use when processing the Service Target.</td></tr>
<tr><td>Escalation - Alerts</td><td>The alert(s) to generate when processing the Service Target.</td></tr>
<tr><td colspan="2">Upcoming Alerts</td></tr>
<tr><td colspan="2">Displays a list of Upcoming Alerts related to this Service Level Target.</td></tr>
<tr><td colspan="2">Current Outage Events</td></tr>
<tr><td colspan="2">Displays a list of Current Outage Events related to this Service Level Target.</td></tr>
</table>

Appendix A: Release and Deployment Management

HP Service Manager uses the Release and Deployment Management application to enable the Release and Deployment Management process.

The following sections shows how you can tailor Service Manager to support Release and Deployment Management as a subset of Change Management.

Release and Deployment Management Overview

The HP Service Manager Release and Deployment Management application, referred to as Release and Deployment Management throughout this chapter, supports the Release and Deployment Management process. It is implemented as a separate category inside the Change Management application and supports and relies on the Change Management process. It ensures that the Configuration Management Database (CMDB) is kept up to date, that changes are appropriately managed, and that all new software and hardware is stored in the Definitive Software Library (DSL) and Definitive Hardware Store (DHS). After one or more changes are developed, tested, and packaged into releases for deployment, Release and Deployment Management is responsible for introducing these changes and managing their release. Release and Deployment Management also contributes to the efficient introduction of changes by combining them into one release and deploying them together.

This section describes how Release and Deployment Management implements the best practice guidelines for the Release and Deployment Management processes.

Topics in this section include:

- "Release and Deployment Management within the ITIL framework" on the next page
- "Release and Deployment Management application" on page 391
- "Release and Deployment Management process overview" on page 392
- "Key performance indicators for Release and Deployment Management" on page 394

Release and Deployment Management within the ITIL framework

Release and Deployment Management is addressed in ITIL's Service Transition publication. The goal of Release and Deployment Management is to plan, schedule and control the build, test and deployment of releases to deliver new or changed functionality, its enabling systems, technology and organization while protecting the integrity of existing IT and Business Services.

Release and Deployment Management includes the assembly and implementation of new or changed services, from release planning through to early life support transition for operational use. It includes, physical and virtual assets, applications and software, training and communication

The purpose of Release and Deployment Management is to:

- Define and agree release and deployment plans with customers and stakeholders
- Ensure that each release package consists of a set of related assets and service components that are compatible with each other
- Ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the CMS and stored in the DML
- Deploy release packages from the DML to the production environment following an agreed plan and schedule
- Ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate
- Record and manage deviations, risks, issues related to the new or changed service and take necessary corrective action
- Ensure that there is knowledge transfer to enable the customers and users to optimise their use of the service to support their business activities
- Ensure that skills and knowledge are transferred to operations and support staff to enable them to effectively and efficiently deliver, support and maintain the service according to required warranties and service levels

The objective of Release and Deployment Management is to ensure that:

- There are clear and comprehensive release and deployment plans that enable the customer and business change projects to align their activities with these plans

- A release package can be built, installed, tested and deployed efficiently to a deployment group or target environment successfully and on schedule
- All aspects that are related within an IT service are considered when creating, building and implementing a new or subsequent release of that service.
- Release activities are repeatable, controllable, scalable and sustainable
- There is minimal unpredicted impact on the production services, operations and support organization

Release and Deployment Management application

The Release and Deployment Management application ensures that the Configuration Management Database (CMDB) is kept up to date, that changes are appropriately managed, and that all new software and hardware is stored in the Definitive Software Library (DSL) and Definitive Hardware Store (DHS). After one or more changes are developed, tested, and packaged into releases for deployment, Release and Deployment Management is responsible for introducing these changes and managing their release. Release and Deployment Management also contributes to the efficient introduction of changes by combining them into one release and deploying them together.

The purpose of Release and Deployment Management is to ensure that all changes are deployed successfully in the least disruptive manner. Release and Deployment Management is responsible for the following functionality:

- Driving the release strategy, which is the overarching design, plan, and approach for deployment of a change into production in collaboration with the Change Advisory Board (CAB).
- Determining the readiness of each release based on release criteria (such as quality of release, release package and production environment readiness, training and support plans, rollout and back out plans, and risk management plan).

Release and Deployment Management offers these benefits for users:

- Provides a packaged release for all changes deployed into production and only deploys changes approved by change management.
- Provides two different types of releases: hardware and software. Once the release type is determined, the application provides the appropriate tasks.
- Ability to manage changes of groups such as Configuration Item (CI) groups and business services.

- Ability to terminate a release at any time except in the Training phase or once it has been installed or verified. At that point you have the ability to back-out the change.
- Availability of optional training phase.

Release and Deployment Management process overview

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

The purpose of Release and Deployment Management is to ensure that:

- Releases follow a set process
- Appropriate users are notified at key points in the process
- Progress of a release is monitored and notification are issued if deadlines are missed
- Releases are supported throughout a simple or complex lifecycle

Release types

Release and Deployment Management includes three release types: Emergency, Major, and Minor. All three release types utilize the Release Management category and workflow in the Change Management module. Additional categories and workflows can be created if required. The steps of the workflow are represented by the phases and tasks within the phase. Service Manager requires that every release has a category and phase, but tasks are optional.

Release phases and transitions

Service Manager uses phases to describe the steps necessary to complete a release. The phase also determine the release screens users see, the approvals required to advance to the next phase, and the conditions that cause the system to issue notification and alerts. Each phase has workflow transitions that control how the release record will move through the workflow. When the work for a given phase has been completed the user will advance it to the next phase. If the release has encountered a failure condition then the release may be move back to an earlier phase for rework or abandoned.

Release tasks

Release Management utilizes tasks to capture work that is necessary for the overall release. This is work in addition to the Change specific tasks that are required to complete the changes that are associated to the release. Examples of required release activities are: determining if funding is available to support the release, arranging for required contracts and licenses, building and delivering training, evaluating the financial impact of the planned release, and performing knowledge transfer after the release has been deployed. Release Models can be used to pre-define task plans for Releases.

Integration with Change Management

In HP Service Manager the Release record and workflow control the overall process of the release, including approvals for the release and the release specific activities (tasks) that need to be complete. The release is related to multiple change requests (RFCs) that have their own workflow, approvals, and tasks. The planning, assessment, build, and deployment of each change is tracked and worked in the Change Management module. The Release provides the higher level oversight and provides visibility into the Change Management process through the Related Records section in the release record.

Release roles

The following table describes the responsibilities of the Release and Deployment Management user roles.

Release and Deployment Management user roles

Role	Responsibilities
Release Manager	• Manages all aspects of the end-to-end release process • Reviews and updates the release policy • Facilitate the bundling of releases • Coordinate planning and preparation for Deployment • Coordinate creation of Deployment Plans • Ensures coordination between the build and test environment team and release teams • Ensures the teams follow the organization’s established policies and procedures • Provides management reports on release progress • Updates the Service Knowledge Management System

Release and Deployment Management user roles , continued

Role	Responsibilities
Release Coordinator	• Registers the release and applies the correct release model and release detail. • Schedules the release according to the plan created previously. • Creates the release tasks required for the release. • Coordinates the Risk and Impact Analysis phase of the release and creates release plan based on the assessment information. • Verifies if the release has passed the test criteria. • Verifies if the release 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.
Release Approver	• Uses the Service Manager tool to Change Advisory Board to approve or deny Releases when requested

Key performance indicators for Release and Deployment Management

The Key Performance Indicators (KPIs) in the following table are useful for evaluating your Release and Deployment 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 Release and Deployment Management

Title	Description
% of release success rate	Percentage of the total number of closed releases successfully implemented in a given period.
% of release defect rate	Percentage of releases resulting in Incidents in a given period.
Number of known release errors	The number of known errors by category by release over time.
% of approved releases that do not result in an incident	Percentage of approved releases that do not result in an Incident in a given period.

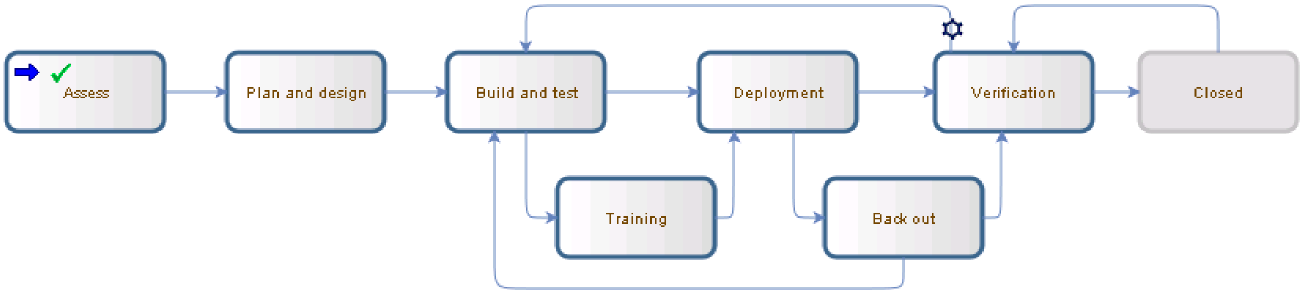
Key performance indicators for Release and Deployment Management, continued

Title	Description
% of releases implemented in the approved release implementation window	Percentage of releases that are completed within the approved implementation window.

Release and Deployment Management Workflow

The Release Management category includes seven phases, which follows the recommended Information Technology Infrastructure Library (ITIL) process by providing you with a set of approvals and tasks that you can expand.

The Release and Deployment Management workflow is illustrated in the following figure:



Release Registration and Assess

Releases may be raised either as the result of advanced planning activities, so they are coordinated with planned maintenance windows, or in response to a change request or group of change requests. The release should contain changes that are planned to be executed together, either because they all affect the same service or because they will be executed during the same release window. During the Assess phase the importance and value of the release should be determined and documented in the release record.

Plan and Design

Plan releases in line with requirements resulting from approved changes. Analyze all the affected Configuration Items (CIs) and CI Groups, review what software or hardware is needed to accomplish the plan, and determine the cost. This phase requires the plan and design approval before going to the next step.

Build and Test

Build effective release packages for the deployment of one or many changes into production. Test release mechanisms to ensure minimum disruption to the production environment. During this phase the individual changes that make up the release will be built and tested in isolation as part of the change management process and the combined release package will be built and tested as well. This phase requires that the build and testing of the release has been approved before going to the next phase.

Training

Identify and fulfill training requirements for various users. This phase is optional and is activated when you select high Impact Assessment and high Urgency for the release change.

Deployment

During the deployment phase of the release the individual changes that make up the release will be implemented in a coordinated fashion in order to maximize the likelihood of success while minimizing the required service disruption. The implementation of each individual change is executed and tracked in the Change Management process.

Back Out

The back out phase is an optional phase that is entered if the release encounters an issue during the deployment phase and the work done for the release must be undone. The work required for back out will have been determined and recorded during the build and test phase.

Verification and Release Closure

After the release is completed, the results must be report for evaluation to those responsible for managing releases and then presented for stakeholder agreement. This process involves analyzing the results for the changes that make up the release and the closing of related user interactions, incidents, and known errors. The verification phase is performed to confirm that:

- The release met it objectives

- The release requestor and stakeholders are satisfied with the results

- Lessons learnt are incorporated in future releases

Release and Deployment Management Details

HP Service Manager uses the Release and Deployment Management application to enable the Release and Deployment Management process.

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

Release and Deployment Management field descriptions

Label	Description
Release ID	This is a system-generated unique value assigned when the release is opened.
Phase	This is a system-generated field that specifies the name of the current phase of the change. For a list of the phases, see "Release and Deployment Management Workflow" on page 395.
Status	The status of the release within the release phase. The status is either initial (the phase has started) or closed (the phase has ended)
Approval Status	This is a system-generated field that defines the global approval status for the change, not for a single approval. The system sets this field depending on current approvals and the approval type defined for the module. These approval statuses are available out-of-box: • Pending • Approved • Denied
Reason for Release	A code that indicates the primary reason for implementing the release. Examples of reason codes are Incident/Problem Resolution and Business Requirement.
Assigned To	The name of the person the release is assigned to.
Release Type	This field indicated the type of release. The release types available out-of-box are: • Major • Minor • Emergency

Release and Deployment Management field descriptions, continued

Label	Description
	This is a required field.
Release Coordinator	The person responsible for coordinating the release implementation. Each Release Coordinator may belong to several assignment groups. Each group must have only one Release Coordinator.
Initiated By	The name of the user requesting the release. 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 release.
Alert Stage	This is a system-generated field that lists the current Alert Stage of this request. This field is updated automatically when alerts are processed against the release. Do not update it manually. The alerts are processed against a release by using the phase definition.
Planned Start	This field specifies the date and time that the work to implement the release should start.
Planned End	This field specifies the date and time that the work to implement the release should end.
Downtime Start	The date and time when the release is scheduled to begin. Scheduled downtime only needs to be filled when the service is down, while implementing the release.
Downtime End	The date and time when the release is scheduled to end. Scheduled downtime only needs to be filled when the service is down, while implementing the release.
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 Downtime Start and 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.
Risk Assessment	Specifies a code that indicates the risk incurred with the implementation of the change. These risk assessments are available out-of-box: • 0 - No Risk • 1 - Low Risk • 2 - Some Risk • 3 - Moderate Risk

Release and Deployment Management field descriptions, continued

Label	Description
	- 4 - High Risk - 5 - Very High Risk After a user selects this field, the release may require additional approvals based on the risk. The approval is based on the risk number in the assessment approval record.
Impact Assessment	This field specifies the impact the release has on the business. The impact and the urgency are used to calculate the priority. These impacts are available out-of-box: - 1 - Enterprise - 2 - Site/Dept - 3 - Multiple Users - 4 - User The out-of-box data is the same as Interaction Management, Problem Management, Incident Management, and Change Management. This is a required field.
Urgency	The urgency indicates how pressing the release 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, problem, and change tickets. For more information, see "Service Desk Interaction Management form details" on page 42. This is a required field.
Priority	This is a system-generated field using the urgency and impact of the release. This field functions similarly to the same field for interaction, incident, problem, and change tickets. For additional information, see "Service Desk Interaction Management form details" on page 42.
Policy / Regulation	This field is used to indicate if the release must follow specific policies or regulations.
Description	Provides a detailed description of the release. This is a required field.
Overall Assessment	A detailed description of the reasons to implement the release. It should be as detailed as possible.
Closure Code	The completion code indicates the way a release is closed. VALID VALUES

Release and Deployment Management field descriptions, continued

Label	Description
	• 1 - Successful • 2 - Successful (with problems) • 3 - Failed • 4 - Rejected • 5 - Withdrawn • 6 - Cancelled
Closing Comments	This field contains comments about the status of the release when it is closed.
Associated CIs	The list of Configuration Items (CIs) affected by the release.
Release Information	The Release Information section records the Products being affected by the Release along with the Package Version of the release.
Backout Method	Provides a detailed method for backing out the release if there is a problem during the deployment phase. This is a required entry during the Plan and Design phase.
Approvals	The Current Approvals section provides an overview of the current approvals related to release 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 the release. Approvals give controlling authorities the ability to stop work and to control when certain work activities can proceed. The data displayed includes the following information: • Approval Type • Approval Status • # Approved • # Denied • # Pending The Approval Log section provides an overview of past approvals related to the release as well as important information such as approval status and approvers. The data displayed includes the following information: • Action • Approver/Operator

Release and Deployment Management field descriptions, continued

Label	Description
	• By • Date/Time The Pending Reviews section provides the name(s) of the groups or operator IDs that should review the release after it has been approved.
Tasks	Whenever a release 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: • Task No • Status • Approval Status • Assigned To • Description • Category
Activities	The Activities section allows users to enter new updates for the record or view journal updates and historic activities for the record. **New Update** • **New Update Type** Specifies or categorizes the activity update; for example, communication with the customer. • **Visible to Customer?** A check box that a user can select to make the update visible to a customer. • **New Update** This field is used to enter notes to explain and describe updates made for the record. If Journaling is enabled, the text entered here displays in Journal Updates. If Activities is enabled, the text entered in this field displays as an activity record for the selected activity type. **Note:** The System Administrator is responsible for enabling Journaling and Activities. **Journal Updates** Journal Updates shows text entered in the New Update field along with a

Release and Deployment Management field descriptions, continued

Label	Description
	timestamp for the update. This field displays information when Journaling is enabled. **Activity Type** To filter the list by the type of activity, select an activity type and click **Filter**. Service Manager opens a new record list to display the records of that activity type. The activities list shows activities for the current record. The activities are listed in order of occurrence, with the newest at the beginning of the list. The following information displays for each activity: • Date/Time • Type • Operator • Description
Test Results	The Test Results section allow you to record the planned release testing activities along with an indicator of whether the test passed or failed and a description of the results of the test.
Attachments	You can use the Attachments section to attach documents to releases. To attach a document to a release: 1. Click **Add File...** in the Attachments section. 2. Use the Specify File Location window to browse for the file. 3. Click **OK**. The selected file appears in the Attachments section. Additional methods to attach files to an incident record with a Windows client include: You can cut or copy a file from a file management utility, or your desktop, and paste it into the Attachments section of a record. You can also cut or copy an attachment from one Service Manager record into the Attachments section of another record. Use a file management utility to open the folder containing the document you want to attach, or select a file from your desktop. Make sure that the Attachments section is open on your screen. Drag the selected file to the Attachments section.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Processes and Best Practices Guide (Codeless Mode) (Service Manager 9.41)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-ITSM@hp.com.

We appreciate your feedback!