Peregrine

ServiceCenter
Introduction and Best Practices

Release 5.1

Peregrine
SYSTEMS

Contents

About this Guide

Welcome to ServiceCenter® *Introduction and Best Practices.* This guide is designed to provide all potential and new users of ServiceCenter with the fundamentals of its features, architecture, and capabilities. No previous knowledge of ServiceCenter is assumed, other than a familiarity with service management and computer basics.

This introduction also identifies other sources of detailed information about ServiceCenter, including the out-of-box workflow for the industry standard in processes and best practices.

Organization

The guide is divided into the following chapters.

- *Change Management* on page 69 — ensures that standardized methods and procedures are used for efficient and prompt handling of all changes to an organization's infrastructure.
- *Inventory Management* on page 91 — enables enterprises to efficiently identify, control, maintain, and verify the versions of configuration items (CI) that exist in the IT infrastructure.
- *Service Level Management* on page 105 — tracks performance of service agreements between customers and service providers.
- *System Set-up and Administration* on page 109 — provides an overview of the range of ServiceCenter utilities and selected files used by system and database administrators for set-up and operation.
- *Tailoring ServiceCenter* on page 121 — introduces the range of ServiceCenter tools for tailoring.
- *Further Information and Support* on page 131 — details the documentation and training courses available from Peregrine Systems. It also provides contact details for Customer Support.
- A *Glossary* on page 137— provides a list of terms and definitions related to ServiceCenter applications, processes, and procedures.

Terms

The following terms are used throughout this manual:

Service call—A call to the help desk that was not immediately resolved and for which an incident ticket has been issued.

Incident—A specific problem that may or may not have a set of related incidents.

Known error—A problem for which the root cause has been diagnosed and a solution or work-around has been determined.

Request for Change (**RFC**)—A request for change to any component of an IT Infrastructure or to any aspect of IT services.

Root cause—The underlying cause of a problem for one or more incidents.

Sample Screens and Examples

The sample screens and examples included in this guide are for illustration only, and may differ from those at your site.

Related Documentation

Available ServiceCenter documentation includes on-line and softcopy guides for installation, system and application set-up and administration, application users, and tailoring. For a complete listing, see *Further Information and Support* on page 131.

Release notes are published for each new version of ServiceCenter, summarizing new features and providing information about how to find out other details related to the release, including the compatibility matrix and any known issues.

For the various operating systems and the third party databases and programs which may be specific to your site, refer to the manufacturer's documentation.

Contacting Education Services

Training services are available for the full spectrum of Peregrine Products including ServiceCenter.

Current details of our training services are available through the following main contacts or at:

http://www.peregrine.com/education

Address:	Peregrine Systems, Inc.
	Attn: Education Services
	3611 Valley Centre Drive
	San Diego, CA 92130
Telephone:	+1 (858) 794-5009
Fax:	+1 (858) 480-3928

1 Overview of ServiceCenter

CHAPTER

ServiceCenter enables companies to manage their service and support operations. It provides the tools and workflows needed to manage corporate assets: the people, knowledge, information, and all tangible resources collectively known as "infrastructure".

Topics in this chapter include:

Enterprise Service Management

ServiceCenter is Peregrine's enterprise service management solution, based on industry standards. Its integrated modules are designed for out-of-box implementation, with best practice work flows that help organizations support their infrastructure and drive competitive advantage in their core businesses.

Architecture

ServiceCenter has a three-tiered client/server architecture:

- Presentation layer, the client through which windows of information are interpreted and displayed to the user. (In ServiceCenter, these displayed windows are known as 'formats' or 'forms', terms used interchangeably.)

- Application layer, comprising the various application modules and the run-time environment (RTE). The application server executes the workflow code.

- Database, either the out-of-box database or an external relational database management system (RDBMS) to which ServiceCenter has been mapped. The application workflow code and the format descriptions are stored in the database.

Presentation Layer

Client   Client   Client   Client

Service Management   Incident Management
Inventory Management   **SC Applications**   Root Cause Analysis
Change Management   Request Management
Contract Management   SLA Management

Oracle   P4
Sybase   **Database**   DB2
SQL Server   Informix
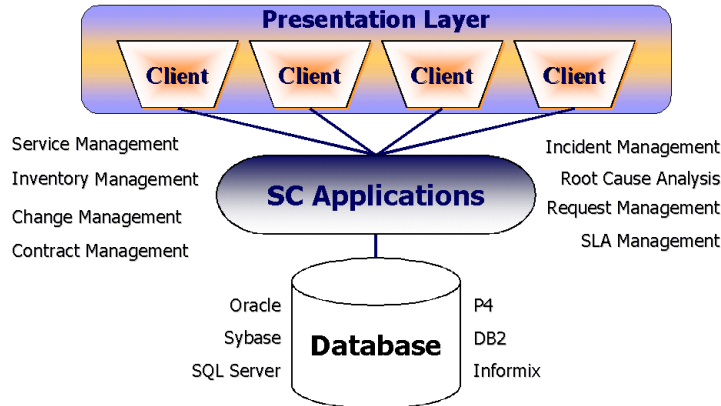
Parameters are set in the ServiceCenter initialization (sc.ini) file to select language, display color scheme of the forms, relational database management system (RDBMS), and for entry of the authorization code to system access.

For a list of possible sc.ini parameters, see *ServiceCenter Technical Reference*.

Run-time Environment (RTE)

The foundation of ServiceCenter architecture is the run-time environment (RTE), the collection of executable programs that interprets the applications and translates application requests into appropriate actions for a specific platform. The RTE runs on both the server and on any client workstation connected to ServiceCenter. RTE functions include:

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

ServiceCenter Clients

The application server retrieves a form from the database and passes it as a block to the client layer. The client interprets the descriptions and builds the form that is displayed on the user's monitor or passed to an interface.

Several types of client are available in ServiceCenter:

- Windows client.
- Java client.
- Text client, SC3270 client.
- ServiceInfo client.
- Computer-telephone integration (CTI) client.

Windows Client

The Windows client is a graphical user interface (GUI) client, available on Microsoft Windows platforms for communicating with a server running on Windows, OS/390, or Unix platforms.

Java Client

The ServiceCenter Java client is a complete and fully functioning Java interface to the ServiceCenter applications, based on the programming language developed by Sun Microsystems and licensed to other vendors, including Microsoft.

The Java client supports the same functionality as the Windows client. In addition, the Java client includes:

- ServiceCenter Explorer, a tree-based navigation window.
- Favorites Bar, similar to that found in Web browsers.
- Frequently used forms.
- Ability to suspend a session, or have multiple sessions.

Since the client is implemented in Java, it can run wherever a proper Java environment is supported. In addition, the client can be configured to run as a stand-alone application, or can run under a Web server so that the client can be downloaded and executed in a Web browser. The Web server location and the Java client's awareness of the Web server are set either at installation or when configuring the HTML files that launch the Java client in a browser.

Features of the Java client include:

- Support of Input Method Editor (IME), a Microsoft feature that enables inline editing of languages with a large number of characters such as Japanese.
- Use of TCP/IP sockets to communicate with a standard ServiceCenter server. The Java client can be installed and put into use without any changes to an existing server environment.
- Provision for an additional security layer, the Server Hub, which is a Java servlet that acts as a proxy to the ServiceCenter server. Instead of connecting directly to the ServiceCenter service, the Java client identifies itself to the Server Hub, which relays information between the client and server.

Advantages of the Java Client

There are several advantages to using the Java client:

- No client-side administration. The Java client downloads upgrade automatically as they become available.
- All ServiceCenter applications are supported without any modifications or customization. The screens can have the same look and feel as they do for Windows clients, or users can use the tree-based navigation menu. Printing functionality is included. Support for file attachments and OLE attachments is also included.

- The growing number of tools and libraries that support Java promise to make this an implementation that can offer the very latest support for sophisticated graphical user interfaces (GUIs).
- Java provides a portable execution environment, allowing Peregrine to support multiple platforms simultaneously.

For details, see the *Java Client Installation and Configuration Guide* and the *ServiceCenter User's Guide.*

Java Client Section 508 Compliance

The Java client has special features implemented in support of Section 508 compliance. For details, see the Accessibility Specifications section of *Java Client Installation and Configuration Guide.*

Computer-Telephone Integration (CTI) Client

ServiceCenter Telephony (SCT) provides options for computer-telephone integration (CTI), so that workstations can be set up to answer incoming telephone calls.

ServiceCenter Telephony uses Microsoft's Telephone Application Programming Interface (TAPI) add-on features as an interface for the 32-bit ServiceCenter Windows client. By clicking on a button with the mouse, a user can answer a call, place a caller on hold, return to a call, or hang-up.

For details about CTI, see the *System Administrator's Guide.*

Text Client, SC3270 Client

The text client performs no processing. The terminal is used only as a display device. Unlike the Windows client, the text client is not a GUI.

A text client can access ServiceCenter running on a Unix system via the SC3270 interface. The SC3270 client enables 3270 terminals to connect to ServiceCenter servers running on non-MVS platforms such as Windows and Unix.

For details, see the *SC3270 Client Installation Guide.*

Integrations with Other Products

Through use of Peregrine integration points, such as SCAutomate, Connect-It and the Federated Database, ServiceCenter can be integrated with a range of other Peregrine and third-party products to provide extensibility to total infrastructure management.

Automation

ServiceCenter integrates with Peregrine's Automation suite to provide network monitoring capabilities, launching applications from within ServiceCenter to gather information about devices or problems.

- Desktop Inventory and Network Discovery automatically populate ServiceCenter device records with data about the various devices on the network.
- When a problem is detected on the network, Network Discovery sends a message to ServiceCenter to automatically open an incident ticket. When the condition has been resolved, ServiceCenter is notified and the incident ticket is automatically closed.
- Desktop Administration can launch specific applications from within ServiceCenter to gather information about a specific device or problem.

Get-Answers

Integrating Get-Answers with ServiceCenter enables help desk operators to search the knowledge base and submit new knowledge entries based on descriptions provided in call records and incident tickets.

ServiceCenter Mobile

ServiceCenter Mobile is an integration with Personal Digital Assistants (PDAs), using the Palm operating system (OS), Windows CE, or PocketPC. It enables ServiceCenter users to:

- Download a selected set of incident tickets to a Palm OS device for reviewing and checking in a mobile environment.
- Update or close incident tickets, using the Palm OS device to synchronize the information back to ServiceCenter.
- Create new incident tickets on the Palm OS device in preparation for uploading the tickets to ServiceCenter's Incident Management when the operator is back at a ServiceCenter workstation.

ServiceCenter's Federated Database

The Federated Database is a logical database that combines data from more than one physical database into a single record that can be viewed and maintained from within ServiceCenter.

It provides true data sharing, with no replication of data. Although the ServiceCenter record is comprised of data from multiple physical sources, any particular field exists in only one physical location.

A typical use of ServiceCenter's Federated Database is for accessing asset and location data from Peregrine's AssetCenter, eliminating the need to maintain duplicate information in each system's database.

Integrations with Third-Party Products

Work Management

Work Management supports comprehensive scheduling, tracking, and reporting functions of the work force. It is designed for organizations seeking to increase productivity by decreasing downtime, improving operator utilization, and enhancing help desk efficiency.

For example, a given help desk department has eight support technicians who are responsible for resolving computer hardware and software problems for 1,000 users. At any given time, there are hundreds of problems, changes, tasks, and requests reported by users waiting in the queue to be resolved. Maximizing the assignment of the limited resources is key to the success of the service.

Work Management's automatic scheduler is designed to assign incidents, changes, tasks, and requests in the most efficient sequence possible, enabling managers to:

- Make assignments according to each operator's capabilities.
- Track how long contacts are kept waiting.
- Determine the overall organizational downtime.

For details, see *ServiceCenter Work Management*.

ReportCenter

ReportCenter is a Windows-based application that provides desktop reporting, enabling users to generate real-time, graphical reports from ServiceCenter data.

ReportCenter uses the Crystal Reports engine. Besides the standard reports that come with ReportCenter out-of-box, the user can create new reports.

For details, see *ServiceCenter ReportCenter*.

Extensibility

Peregrine's SCAutomate and Connect-It integration points provide extensibility to ServiceCenter through interfaces to leading products such as enterprise resource planning (ERP), network system management tools, computer telephony, FAX, email, pager, and other systems.

ServiceCenter Applications

ServiceCenter modules enable out-of-box workflow for service management. These modules work together to process a reported incident through restoration of service, analysis and, when necessary, changes to the IT infrastructure.

ServiceCenter's integrated applications are designed for ease-of-use and management of interrelated events that occur throughout the service life cycle of an asset. Additional applications optimize productivity and improve cost controls.

Service and Incident Management

Service and Incident Management is also referred to as the help desk process in the IT infrastructure. When a call comes in to the help desk, the call details are recorded and monitored in the Service Management module. After the call details are analyzed and it is determined that an immediate solution is not available, an incident ticket is opened. Incident tickets are then handled in the Incident Management module.

Service Management (SM)

The Service Management module is the entry point for enterprise service management, enabling help desk operators to document and track all incoming calls.

Service Management provides one-button access to other ServiceCenter applications for automatically entering information received in the call. With Service Management, help desk operators can:

- Take new calls (including emails), recording details and creating a call report. Reminders can be set up for follow-up at a specific date and time, along with required actions. Calls can also be recorded automatically.
- Use pre-defined inboxes for organizing and checking their workloads.
- Search the knowledge base for answers to queries and additional technical information.
- Check and search lists of call reports, incident tickets, and change management records.

For details about Service Management, see *Service and Incident Management* on page 35, the *User's Guide*, and the *Application Administration Guide*.

Incident Management (IM)

The primary goal of Incident Management is to restore service operation as quickly as possible, minimizing the impact on business operations. Incident tickets are opened when the problem cannot be resolved in the call that was opened via Service Management.

Incident Management enables help desk operators to report and track reported incidents. Once problems are recorded, support technicians are assigned incident tickets for resolving the issues. Automated notification and escalation procedures support tracking and fast resolution of the problem, enabling infrastructure users to be back to work as soon as possible.

Generated reports show trends, enabling management to take a proactive action in managing the company's infrastructure.

With Incident Management, incident tickets are:

- Created and opened by help desk operators, or automatically by an interface with other systems via ServiceCenter's Event Services. The information required on the incident ticket depends on the category assigned to it, according to the reported problem.
- Sent automatically to the ServiceCenter inbox of personnel (for example, a technician) in the appropriate assignment group. Queries enable personnel to search for specific tickets and status, as well as view related call reports. The knowledge base can be searched for related information.
- Tracked, updated, and resolved by personnel and managers. ServiceCenter can automatically send notifications when an incident ticket is not updated within a specified time period. The urgency of the ticket can be escalated automatically, based on a series of alerts. Priority of the ticket is based on business need.

When the incident ticket is resolved, the resolution can be emailed or faxed to the user who reported the incident. Cause and probable cause codes can be assigned to incident tickets for reporting and tracking. Root cause tickets can be opened from incident tickets if there is a need to investigate an underlying cause for one or more incidents.

The goal of Incident Management is to restore service efficiently and keep the impact on business operations to a minimum. By following Incident Management best practices you:

- Provide incident control.
- Notify the right people of critical events.
- Keep Service Level Agreements in good standing.

Incident Management reduces operational risk, automates time-consuming tasks, and enables proactive IT Infrastructure Management. For details about using and setting up Incident Management, see *Service and Incident Management* on page 35, the *User's Guide*, and the *Application Administration Guide*.

Root Cause Analysis (RCA)

Root Cause Analysis implements ITIL's Problem Management to find permanent solutions for underlying problems that cause incidents. It also helps minimize the adverse impact of incidents in the IT infrastructure by identifying the root cause. It promotes proactive management to avoid future incidents.

- When an incident ticket is created, the help desk operator can check the database for known error tickets or find out if the problem matches one already recorded in the Root Cause Analysis (RCA) database. If no match is found, a new root cause analysis record can be opened.
- As the support team works to assess the cause, RCA is used to track the root cause record for future searches. The team implements the solution and notifies the original caller.
- Root cause analysis records can be opened and updated. Reminders can be set for automatic notification for follow-up. Related incident records can be associated with the root cause record, as well as change requests.
- If a work-around solution is found, the root cause ticket can be changed to a known error, accessible through database searches by the help desk staff when creating new incident tickets.

- When a solution has been identified, the known error record is closed. Part of the solution may include improvements to documentation, training, and support procedures.
- As in other modules, tickets are automatically sent to the inboxes of appropriate personnel and managers. Extensive searches of the database and knowledge base support the investigation, tracking, and resolution of the underlying problems.

The main goal of Root Cause Analysis is to reduce the number of incidents by locating and finding solutions to repeated problems within the infrastructure. If Root Cause Analysis is successful, the number of calls to the help desk will be reduced.

Through Root Cause Analysis best practices, you:

- Take measures to prevent failures.
- Identify the underlying causes of issues within the infrastructure.
- Create known errors to document potential solutions.

Root Cause Analysis links with both Incident Management and Change Management.

For details about using and setting up Root Cause Analysis, see *Root Cause Analysis* on page 61, the *User's Guide*, and the *Application Administration Guide.*

Change Management (CM)

Change Management ensures that standardized methods and procedures are used for efficient and prompt handling of all changes to an organization's infrastructure.

The goal of Change Management is to minimize the impact of changes on the quality of service. Typically, a change has been identified as part of the resolution of incident tickets or for resolving root cause records and known errors. Changes such as upgrades to central servers or network installations often impact several users.

By its out-of-box workflow, Change Management enables personnel and management to:

- Create a request for change (RFC) ticket, assigning a unique number against which all activity can be tracked and reported. Changes are classified by categories, including default categories such as HW (hardware), and MAC (general purpose move/add/change). Site-specific categories can also be defined.

- Within a change record, identify the tasks (work processes) required to accomplish the change. The system can automatically notify those responsible for accomplishing the tasks. Inboxes provide a convenient way for technicians to manage their workload. Tasks are also assigned categories to facilitate tracking, reporting, and assignment.

- Follow, track, and query on a standard workflow through the entire implementation cycle. Phases are groupings of activities within a task or change that identify the logical sequence of repeatable steps within the change implementation cycle. Typically, an RFC might have four phases:

  - Assessment phase - for opening and approving the RFC.
  - Building phase - for assigning the person who is actually implementing the change.
  - Testing phase - for recording the test data and the testing results for the change. If the test fails, the phase automatically reverts back to the Build phase.
  - Implementation phase - assuming success in testing, the change can be implemented. Details of the implementation can be recorded, including a review process that documents the success or failure of the change.

Change Management provides the tools to effectively initiate and manage change in the infrastructure. Changes are managed in a controlled way that will solve the problems identified through the Root Cause Analysis process. In this way, known errors are eliminated and the number of incidents is reduced.

The Change Management process helps you to:

- Minimize operational risk.
- Maximize the benefits of change.
- Provide a repeatable and automated process for Infrastructure Management.

For details about using and setting up Change Management, see *Change Management* on page 69, the *User's Guide*, and the *Application Administration Guide.*

Request Management (RM)

Request Management (RM) provides a point of entry for employees to request goods and services. It automates the ordering, manager approval, and tracking of assets, from requesting, ordering and procurement to delivery and installation.

Request Management is based on catalogs, lists of parts and services that requestors can order. Out-of-box catalogs include request category packages, logical bundles of items that facilitate the initial request and ordering, such as a Employee Setup.

For example, the catalog enables the hiring manager to select a predefined set of hardware, software, and services appropriate for the new employee by selecting the Employee Setup item. This single item then automatically initiates orders for the components within the new employee setup item. Individual line items can be added or changed as required. The manager can then track each component of the order.

Request Management phases determine how quotes, orders, and line items are processed, controlling the activity allowed during each administrative step in the workflow process. This might include, for example:

- Initial phase, for setting up the quote, with approvals processing.
- Ordering phase, for order generation.
- QA phase, for verifying successful fulfillment.

The approval process automates and formalizes the evaluation of quotes and orders by the appropriate management. Approvals trigger workflows, moving automatically to the next phase.

Request Management can automatically send alerts and messages, notifying requestors and other users of pending quotes, orders, and the status of requested items through the life cycle.

For details about using and setting up Request Management, see the *Request Management Guide*.

Inventory Management (ICM)

Inventory Management (also known as Inventory and Configuration Management (ICM)) enables enterprises to efficiently identify, control, maintain, and verify the versions of assets/configuration items (CI) that exist in the IT infrastructure.

Inventory Management helps track software and hardware components and their relationships in the network by creating records about devices, service information, and software. For example, a network administrator can call up a list of the PCs for the entire site.

All assets are defined in the device file, the foundation of Inventory Management. Asset records can include contact, location, vendor, and outage history information. Other ServiceCenter applications, such as Incident Management and Change Management, access ICM's repository of data in the inventory files to populate fields on forms through the use of link records.

Inventory Management is the process you use to record the location and status of each asset. This includes documenting any changes made to these assets and providing this information for other departments within the company. You can use Inventory Management to assign assets to contracts, as well as reconcile licenses to verify software compliance.

Inventory Management forms the foundation of service management by helping you to:

- Identify detailed information about resources and their relationships.
- Control your infrastructure changes.
- Keep resource information updated and accurate.

For details about Inventory Management, see *Inventory Management* on page 91, the *User's Guide*, and the *Application Administration Guide*.

Service Level Management (SLM)

Service Level Management enables IT organizations to align the services provided with the entitlement, availability, and response time needs of each business unit.

Service Level Management comprises Service Level Agreements (SLA) and Service Contracts.

Service Level Agreements (SLAs)

Service Level Agreements help to:

- Allocate resources effectively.
- Measure performance to increase quality of service.
- Lower IT infrastructure support costs.

For details about using and setting up Service Level Management, see *Service Level Management* on page 105 as well as the *Request Management Guide*.

Service Contracts

Service Contracts are integrated with Service Management, Incident Management, Change Management, and Request Management to track labor costs related to providing services to fix an incident.

Service contracts are agreements between a customer and service provider. The contracts compile individual expenses and costs for the applicable incident ticket, change request, or service request.

For details about Service Contracts, see the *Application Administration Guide*.

Scheduled Maintenance

Scheduled Maintenance facilitates the definition and scheduling of recurring maintenance tasks that support an organization's infrastructure. It enables proactive reduction of unplanned outages and system failures by ensuring timely review and care of all service assets across the organization.

Scheduled Maintenance enables service providers to:

- Create and store maintenance tasks.
- Generate and distribute maintenance requests at appropriate times.
- Execute and track maintenance tasks.

Integrated with other ServiceCenter applications, Scheduled Maintenance can automatically generate the appropriate incident tickets, change requests, or Request Management quotes.

For details about Scheduled Maintenance, see the *Application Administration Guide* and the *User's Guide*.

Sample Data

ServiceCenter's sample data can be used as a model for setting up actual site-specific data and to support training. ServiceCenter documentation utilizes the sample data to illustrate the applications and processes described.

The sample data records can be modified or deleted. New ones can be created as required for site-specific situations.

Operator Profiles, User Roles, and Application Profiles

Standard out-of-box operator profiles can be used as templates to facilitate setting up operator access.

Once the system administrator has granted an operator access to ServiceCenter via the operator record, application-specific functionality can be assigned by selecting application profiles.

Sample user roles with standard profiles provide templates for setting up typical access for operators within a given application module. User roles are a convenient way for application administrators to assign profiles to a category of users.

Inventory

A simulated network inventory is included as part of the standard system. The sample inventory database includes modems, PCs, workstations, mainframe hosts, and other types of devices.

Call Reports and Incident Tickets

Sets of sample call reports and incidents are included as part of the standard system. These can be reviewed, updated, and closed as part of system training.

Change Requests

The sample database includes change requests that can be approved and given appropriate user level (for example, administrator).

Quotes and Orders

Request Management has streamlined processes with out-of-box quotes, orders, standard alerts, and approvals. It provides automated ordering, manager approval, and tracking of assets through the different phases of their life cycle — from requesting, ordering and procurement to delivery and installation.

Sample ServiceCenter Process Flow

This example is provided as one possible process flow using ServiceCenter and following ITIL processes. The example follows a user's call to the help desk, through the incident ticket and incident phases, and ends with an RFC being implemented to fix the incident reported by the user.

Sample out-of-box workflow:

1 A user calls the help desk and a call report is opened in the Service Management module.

Note: It is recommended that you use Service Management to track all user calls to the help desk, even if no further action is needed after the call is completed. This ensures that accurate metrics are kept and that all trends within the IT infrastructure are identified.

2 If the reason for the call is a disruption in service and the help desk agent cannot resolve the incident or problem immediately, it is escalated and tracked within the Incident Management module until service is restored.

3 A solution to the disruption in service is found, service is restored, and the incident ticket is closed.

4 When the incident has been resolved, the agent has the option of opening a record in Root Cause Analysis. This would indicate that a possible underlying issue within the infrastructure is the cause of the incident.

5 A specialist reviews the incident record and analyzes the infrastructure to determine the root cause.

6   When the root cause is discovered, the root cause record is closed and a known error record is created. This documents the root cause so that if similar incidents are reported, the troubleshooting process does not have to be repeated. The solution to the known error will also be recorded and used to initiate a request for change (RFC).

7   An RFC is opened so that a permanent fix can be applied to the problem in a controlled and risk-free manner. This is a crucial step in bringing the infrastructure closer to meeting the ITIL goal of reduced incidents.

8   The RFC goes through the appropriate approval process.

9   If the RFC is approved, a qualified person (the change owner) is assigned to ensure that the work is completed.

10   The work performed to fix the problem is tested to make sure that the fix has taken care of the reported incident.

11   The RFC is closed.

Common Practices

ITIL-Compliance

ServiceCenter's built-in and tailorable workflow is based on industry best practices, compliant with the Information Technology Infrastructure Library (ITIL). ITIL standards have become a widely recognized source of guidelines for information technology service management.

Using best practices eliminates trial and error. It organizes service management around business solutions with higher productivity. ServiceCenter provides out-of-box workflow, resulting in less time designing and developing tools, and more time supporting business operations.

Processes and Best Practices

ServiceCenter applications incorporate best practice workflows in standard format designs and field definitions, providing out-of-box solutions to streamline implementation and minimize the initial implementation. Additionally, sample data and ServiceCenter Best Practice Delivery provide guidelines for best practice.

This guide documents the ITIL-compliant workflows that are standard with out-of-box ServiceCenter applications. It includes high-level workflow diagrams and step-by-step guidelines.

ITIL processes provide a framework with which you can identify, record, and control all of the objects that make up an information technology (IT) infrastructure. The IT infrastructure is comprised of a variety of objects and processes including equipment, software, documentation and people.

The out-of-box workflow is based on this industry standard. ServiceCenter provides organizations with a way to manage their IT infrastructures. Breakdowns are minimized and any incidents that occur are quickly analyzed and fixed.

The goal is to find permanent solutions for incidents and to ensure that the infrastructure is being managed in a manner consistent with business goals—the right services provided for the right costs.

Service Wisdom

Service Wisdom is a comprehensive set of service management best practices and processes, presented in a Web browser-based format. It has been developed from original material by Malcolm Fry, an industry leader in IT service management.

Service Wisdom provides ITIL-based best practice workflows for processes and stages, as well as activity details, for:

- The Service Desk and Incident Management. This process corresponds to ServiceCenter's Service Management module and Incident Management module.

- Problem Management. This process corresponds to ServiceCenter's Root Cause Analysis module.
- Change Management. This process corresponds to ServiceCenter's Change Management module.

Language Support

Language support for ServiceCenter has two levels: enablement and localization.

Global Service Management

ServiceCenter's distributed service management capability makes it possible to deploy a global support operation. A range of localized ServiceCenter versions are available at user login.

Enablement

When ServiceCenter is enabled for a language, users can enter and retrieve data, and create forms and messages using the appropriate keyboard or other means of entry.

Besides English, ServiceCenter is enabled for:

- All languages that use the Latin I code page
- Chinese, both Simplified and Traditional
- Cyrillic
- Greek
- Japanese
- Korean
- Polish
- Thai

Important: Entering data into ServiceCenter in a language that is not supported can result in corruption of that data.

For details about language support, contact Customer Support (see *Contacting Customer Support* on page 135).

Localized ServiceCenter Versions

Localized versions of ServiceCenter have been enabled for the language, plus the out-of-box forms have been translated. They will display in the localized language, assuming that the language has been set up by the system administrator.

Localized versions of ServiceCenter let sites and users select the language in which their system displays by selecting from a drop-down list when they log into the system. This selection determines the language for the forms, messages, and help text that will be displayed for their session.

Language Set-up

The system administrator sets up language support by setting the appropriate system parameters in the sc.ini file. The language parameter defines the code page to be used, controls the way the data is displayed, and determines how typed-in data is interpreted. The server runs the code page defined in the sc.ini file. This, in turn, determines the code page used for the database.

The default language for a given user can be set up by the system administrator to be different from that of the system's default language. The user-specific definition is set up in the sc3user.ini file.

Localized Versions Groups

Localized versions come grouped according to the code page they use. Current groupings available or planned include:

- English, French, Italian, German, Spanish, Brazilian Portuguese.
- English, Japanese.
- English, Polish.

The timing and availability of localized versions vary by release and language. For details about specific requirements, see *Contacting Customer Support* on page 135.

2 Service and Incident Management

CHAPTER

This chapter discusses best practices for the Service and Incident Management process. The main function of Service Management is to monitor, track, and record calls and incidents. The main function of Incident Management is to resolve incidents and restore normal service operation as quickly as possible.

Topics in this chapter include:

Introduction

Service and Incident Management provides total incident control. This ensures that:

- Calls are logged and monitored.
- Incidents are resolved quickly.
- Solutions minimize risk and negative impact on your infrastructure.
- Information for trend analysis is available.
- Open incidents are automatically linked to related records and modules.

Incident Management automates incident management workflow based on key business rules, ensuring that the right people are notified of critical events and that service level agreements stay in good standing.

Service Management (SM)

The Service Management module is the entry point for enterprise service management, enabling help desk operators to document and track all incoming calls.

Service Management provides one-button access to other ServiceCenter applications for automatically entering information received in the call. With Service Management, help desk operators can:

- Take new calls (including emails), recording details and creating a call report. Reminders can be set up for follow-up at a specific date and time, along with required actions. Calls can also be recorded automatically.
- Use pre-defined inboxes for organizing and checking their workloads.
- Search the knowledge base for answers to queries and additional technical information.
- Check and search lists of call reports, incident tickets, and change management records.

For further details about using and setting up Service Management, see the *User's Guide* and the *Application Administration Guide*.

Incident Management (IM)

The primary goal of Incident Management is to restore service operation as quickly as possible, minimizing the impact on business operations. Incident tickets are opened when the problem cannot be resolved in the call that was opened via Service Management.

Incident Management enables help desk operators to report and track reported problems. Once problems are recorded, support technicians are assigned incident tickets for resolving the issues. Automated notification and escalation procedures support tracking and fast resolution of the problem, enabling infrastructure users to be back to work as soon as possible.

Generated reports show trends, enabling management to take a proactive action in managing the company's infrastructure.

With Incident Management, incident tickets are:

- Created and opened by help desk operators, or automatically by an interface with other systems via ServiceCenter's Event Services. The information required on the incident ticket depends on the category assigned to it, according to the reported problem.
- Sent automatically to the ServiceCenter inbox of personnel (for example, a technician) in the appropriate assignment group. Queries enable personnel to search for specific tickets and status, as well as view related call reports. The knowledge base can be searched for related information.
- Tracked, updated, and resolved by personnel and managers. ServiceCenter can automatically send notifications when an incident ticket is not updated within a specified time period. The urgency of the ticket can be escalated automatically, based on a series of alerts. Priority of the ticket is based on business need.

When the incident ticket is resolved, the resolution can be emailed or faxed to the user who reported the incident. Cause and probable cause codes can be assigned to incident tickets for reporting and tracking. Root cause tickets can be opened from incident tickets if there is a need to investigate an underlying cause for one or more incidents.

For further details of using and setting up Incident Management, see the *User's Guide* and the *Application Administration Guide*.

Scope

The activities within the scope of Service and Incident Management guide you through the full lifecycle of an incident, from the user's call to the incident's resolution.

Activities included in Incident Management are:

- **Incident detection and recording**

  The help desk monitors the incident resolution process. The help desk analyst supplies a work around when applicable. The three main functions of this activity are:

  - Incident recording - record the basic incident details.
  - Incident handling - perform initial incident analysis.
  - Escalation - assign incident to assignment group.

- **Classification and initial support**

  The help desk is the central point of contact and the starting point for recording all calls and incidents. The help desk provides the following initial support:

  - Classifies the incident.
  - Matches it against possible known errors.
  - Assigns both impact and urgency.
  - Assesses related configuration details.
  - Gives initial support - provide quick fixes if applicable.
  - Escalates incidents to the appropriate specialist group.

- **Investigation and diagnosis**

  Once an incident has been escalated to an assignment group, the assignment group begins to work toward a resolution. The assignment group:

  - Assesses the incident details.
  - Collects and analyze all related information.
  - Identifies possible resolutions.
  - Updates incident details.

- **Resolution and recovery**

  The assignment group is responsible for the incident's resolution. The assignment group:

  - Resolves the incident.
  - Opens a request for change (RFC) when the incident cannot be resolved.
  - Takes recovery actions. Recovery action is either a permanent solution, a work-around, or temporary fix.
  - Notifies the help desk that the incident is resolved.

- **Incident closure**

  The help desk ensures that the classification of the incident is complete and that, when necessary, the incident was matched with its corresponding RFC. After resolution of the incident, the help desk:

  - Confirms the incident resolution with the originator.
  - Updates the incident status to "closed".

- **Incident ownership, monitoring, tracking and communication**

  The help desk is responsible for incident ownership. The help desk:

  - Monitors all incidents.
  - Escalates incidents when necessary.
  - Maintains communication with the incident's originator.

When a failure occurs or a user needs support, the user is required to make contact with the help desk.

The help desk must capture details of the call and enter them into the proper fields in ServiceCenter. This includes categorizing the call, which can help to diagnose the cause of the issue.

If the help desk successfully resolves the call, the call log is closed.

If the help desk cannot immediately resolve the call, an incident ticket is opened. Here, the category automatically routes the incident to the appropriate support unit and a default severity code is given.

Incident categories

Incident categories are defined up to 4 levels. This allows for greater granularity in defining the incident. It also ensures that the most appropriate severity level is entered and that calls are analyzed effectively.

The level of severity determines the service level that is assigned to the resolution of the incident.

Out-of-box Categories

The following table describes the out-of-box high level categories:

Category	Description
Business Applications	Incidents involving the business application code involving the distribution of software to client systems or distributed servers.
Client System	Incident involving either a single user or user group. A client system can be the physical PC, laptop, PDA or external peripheral or the applications that reside on them.
Enquiry	Incident involving a single user or user group that requires assistance but with no direct impact on the business. An example of this is a request for information.
Network	Incident involving the data communications infrastructure.
Other	Incident that cannot be defined by another category.
Printing	Incident involving the hardware, software or consumable such as toner and paper relating to a printer.
Security	Incident involving the security policy or protection mechanism. This would include anti-virus software problems; "out-off-hours" access to client premises or password problems.
Shared Infrastructure	Incident involving the hardware, operating system, or location of an item of shared infrastructure, other than the communication network.
Telecoms	Incident involving the hardware, operating system, or location of an item of shared infrastructure within the communication network.

Assignment Groups

The following table defines the main out-of-box assignment groups.

Assignment Group	Definition
AUTO	Default assignment group for automation issues.
CLIENT SECURITY	Default assignment group for security issues.
DEFAULT	Assignment group when no other assignment group is specified.
DUTYMANAGER	Default assignment group for duty manager support issues.
FACILITIES	Default assignment group for facilities-level support
FIELD ENG.	Default assignment group for support utilizing field engineering resources
FIRSTLINE	Default assignment group for first line support issues.
HELPDESK	Default assignment group for the help desk
LAN SUPPORT	Default assignment group for LAN support issues
M/F SUPPORT	Default assignment group for mainframe support issues.
ONSITE SUPPORT	Default assignment group for support required on customer sites
PROCUREMENT	Default assignment group for procurement support issues.
REPLACEMENT	Assignment group when a whole unit temporary replacement is required
SECONDLINE	Default assignment group for second line support issues.
SERVICE MANAGEMENT	Default assignment group for Service Management support issues.
SOFTWARE	Second line software support
SYSTEMS ADMIN	Assignment group for system administration issues
SYSTEMS SUPPORT	Default assignment group for issues requiring remote support of systems
TELECOMS	Default assignment group for telecom issues
TRAINING	Default assignment group for training issues
WAN SUPPORT	Default assignment group for WAN support issues

Assigning Incident User Priority

The help desk assigns the severity to an incident. The severity given to an incident is an important part of the incident's resolution because it indicates the priority, or the order in which incidents should be resolved. A level 1, or critical incident, should be investigated and resolved first. However, a level 5, or very low incident, should be resolved first if it is a quick fix.

Severity is assigned by assessing the impact of the incident and the urgency of the incident.

Impact—The degree of the business disruption.

Urgency—How quickly the incident must be resolved.

Severity definitions are as follows:

Level 1 - Critical—(Severe Business Disruption) The business unit or sub-unit is unable to operate; critical system component failed or severely impaired

Level 2 - Major—(Major Business Disruption) Critical user or user group unable to operate, or the business unit is experiencing a significant reduction in system performance

Level 3 - Medium—(Minor Business Disruption) A single user is unable to operate with no available work around

Level 4 - Low—(Minor Disruption) A single user or user group is experiencing incidents, but work around is available.

Level 5 - Very Low—(Inquiry) Single User or User group requiring assistance, but with no direct impact on business, such as a request for information.

Escalating an Incident

Escalation of an incident can be either functional or hierarchical. Functional escalation of an incident is based on competence. Hierarchical escalation is based on authority.

Functional escalation mainly occurs when there is a lack of knowledge or expertise. This requires the incident to be passed from first-level support to second-level support.

Hierarchical escalation can happen during any phase of the incident's resolution. It usually occurs when it appears that the incident is not going to be resolved in a timely manner. The incident should be escalated to a higher authority before the agreed-upon service level time lapses.

Service and Incident Management Workflow

There are six phases of the Service & Incident Management workflow. Each phase contains a number of steps to follow before proceeding to the next phase.

Phase 1: Receive Call

The Receive Call phase deals with incoming calls to the help desk. The following steps guide the help desk through receiving and routing the call.

The following steps are performed by the help desk.

1 Take call.

Determine response time according to the Service Level Agreements (SLAs).

2 Is the call related to an open call?

- Open Call - proceed to step 3
- New Call - skip ahead to step 5

3 Is the call related to an existing call or an existing request for change?

- Call - Retrieve the call number. The call number is in the format: CALL12345.

  - When no call number is given, search for open calls by the contact's name. The search screen is shown below.

Figure 2-1: Search for Call Tickets Form

  - Proceed to Phase 2: Log Call *Existing Calls*
- RFC - Ask the user to provide the RFC number.

  - If no number is given, retrieve number through a criteria search.

4 Update the RFC:

  - If the user is just seeking information, provide the information and end the call. No record of the call is required.

  - If the user supplies an update to the request for change, update the call and transfer the text to the RFC.

- If the new caller is seeking information or updating an existing RFC, create a new call and *link* it to the relevant RFC.

- End call.

5 Open the **New Call** form(cc.incquick.g). For field level details, see *Table 1: New call--Call Detail tab (cc.incquick.g)* in the Field-Level Details section of the *Application Administration Guide.*

Figure 2-2: New Call Form

a Is the user entitled to service? Entitlement is determined by:

- The component being supported: warranties and contracts.
- A valid user.
- A valid contract.

  If the user is *not* entitled to service, notify the user and end the call.

  If the user is entitled to service, determine the call type and check the validity.

- The help desk agent and caller agree on the call type. (Invalid call types would be if the printer needs paper or if there is a need for an RFC). During the call, the help desk and the caller establish whether there is an incident, if it is in scope, and the nature of the incident.

b Is the call a valid call?

- No - notify the user and end the call.
- Yes - proceed to Phase 2: Log Call *New calls*

Receive Call Workflow (Phase 1)

```
                    ┌──────────┐
                    │  Start   │
                    └─────┬────┘
                          │
                    ┌─────┴────┐
                    │ Take call│
                    └─────┬────┘
                          │
                     ◇ Open Call? ◇ ──yes──→ ◇ Existing call or ◇ ──RFC──→ ┌─────────────┐  ┌────────────────┐  ┌──────────┐
                          │                     request for              │ Obtain       │  │ Open and update │  │ End call │
                          │                     change?                  │ details via  │  │ request for     │  └──────────┘
                         no                        │                     │ supplied RFC │  │ change &        │
                          │                       call                   │ number       │  │ update user if  │
                          │                        │                     └─────────────┘  │ required.       │
                  ┌───────┴──────┐            ┌─────┴─────┐                                └────────────────┘
                  │ Open log &   │            │ Phase 2;  │
                  │ take basic   │            │ Log Call  │
                  │ user details │            │ Existing  │
                  └───────┬──────┘            │ calls     │
                          │                   └───────────┘
                  ◇ User entitled to ◇ ──no──→ ┌──────────┐ ──→ ┌──────────┐
                     service?                  │ notify   │     │ End call │
                          │                    │ user     │     └──────────┘
                         yes                   └────┬─────┘
                          │                         ↑
                  ┌───────┴──────┐                  │
                  │ Determine top│                 no
                  │ level call   │                  │
                  │ type and     │                  │
                  │ check        │                  │
                  │ validity     │                  │
                  └───────┬──────┘                  │
                          │                         │
                   ◇ Valid call? ◇ ─────────────────┘
                          │
                         yes
                          │
                  ┌───────┴──────┐
                  │ Phase 2;     │
                  │ Log Call     │
                  │ New calls    │
                  └──────────────┘
```

Phase 2: Log Call

The log call phase is handled by the help desk. All calls must be logged, whether the call is a new call, or an update to an existing call. The subsequent section details logging a new call. For details on updating an existing call, skip to the next section, *Phase 2—Log Existing Calls*.

To log a new call:

1 Complete the call details.

- Fill in all required fields. Required fields are marked with a red triangle in the upper left corner of the field. For field-level details, see *Table 1: New call--Call Detail tab (cc.incquick.g)* in the Field-Level Details section of the *Application Administration Guide*.

  The following fields are required for this step:

  - Contact Name
  - Category
  - Subcategory
  - Product Type
  - Problem Type
  - Assignment
  - Severity
  - Site Category
  - Company
  - Description

  Validation is carried out on all required fields. Fields that are greyed out are read-only and are filled automatically, based on the content of other fields.

  Important validations are as follows:

  - Only valid categories and associated sub-categories, product types and incident types can be entered.
  - The SLA is built from the "Severity" and the "Site Category" and is calculated in Format Control (the "Projected SLA" on the screen may be incorrect until the call is saved). For information on the out-of-box site categories, see *Site category definitions* on page 108.

- The SLA will automatically increase to a higher level if the call being reported has a severity of "Total Loss of Service", if the reporting person is a "Critical User", or if the asset is a "Critical Asset".
- The description form is free-form text and is validated only for presence, not content.

2 Determine the call category.

The four level call categorization is critical and enables:

- Incidents to be passed between desks.
- Incidents to be passed to the right support group.
- Data to be mined for consistent RCA.
- Generation of standardized reports.

3 Update the log record.

Note: For password resetting, follow the SLA's rules for identifying the caller.

Phase 2—Log Existing Calls

Existing calls are logged and updated in the cc.incident.g form. For field-level details see *Table 3: Existing call--Update tab (cc.incident.g)* in the Field-Level Details section of the Application Administration Guide.

To log an existing call:

1 Retrieve the existing call records. Check for all calls with similar underlying problems by using **Option**>**Related**>**Calls**.

2 Establish whether the call is a new call or an update.

3 Provide the user with desired details and log the enquiry.

4 Update the log with the caller's information and notify.

Update the call and transfer items to the incident.

If the caller asks to close the call, update the linked incident records. If there are no other linked calls, change the status to resolved.

Log Call Workflow (Phase 2)

Log New Calls

```
Phase 1
Receive
Call
   │
   ▼
┌────────────┐
│Complete all│
│ call       │
│ details    │
└────────────┘
   │
   ▼
┌────────────┐
│Determine   │
│ call       │
│ category   │
└────────────┘
   │
   ▼
  ╱╲
 ╱  ╲         ┌──────────┐              ╱╲              ┌──────────┐
Is call for   │Check user│             ╱  ╲            │Inform user│
password  ─yes│ identity │─────────── Did      ──no───│of          │
reset?        └──────────┘           authentication   │authentication│
  ╲  ╱                               pass?            │failure     │
   ╲╱                                 ╲  ╱             └──────────┘
   │                                   ╲╱                   │
   no                                   │                   ▼
   │            ┌──────────┐           yes            ┌──────────┐
   └───────────│Update log │◄──────────┘              │ End call │
               │ record    │                          └──────────┘
               └──────────┘
                    │
                    ▼
               Phase 3
               Initial
               Analysis
```

Log Existing Calls

```
Phase 1
Receive
Call
   │
   ▼
┌────────────┐
│Retrieve    │
│ call &     │
│ incident   │
│ records    │
└────────────┘
   │
   ▼
  ╱╲
 ╱  ╲          ┌──────────────┐           ┌──────────┐
Is call for an │Provide user  │           │ End call │
update or  ─Enquiry│with requested│────────│          │
enquiry?       │details and   │           └──────────┘
  ╲  ╱         │log enquiry   │
   ╲╱          └──────────────┘
   │
Update
   │
   ▼
┌────────────┐
│Update log  │
│with user   │
│information │
│and notify  │
│SDU         │
└────────────┘
   │
   ▼
┌──────────┐
│ End call │
└──────────┘
```

Phase 3: Initial Analysis

1 Attempt 1st level diagnosis. Can incident be solved by 1st level diagnosis?

Make the diagnosis within set time scales. The time scales for 1st level diagnosis should be determined by the Service Level Agreement.

- Yes - Provide the caller with the incident resolution.
  - Validate and update relevant categories. If the solution differs from the original description of the incident, revise the call category. ServiceCenter marks the call as fixed during first call.
  - Update the call log.
  - End the call.
- No - Use the **Notify By** field to set the call-back flag.

2 Use **Options** >**Related**>**Incident** to determine if the call is related to an open incident. Is call related to an open incident?

- Yes - Link the call to the associated incident: use **Options** >**Related**>**Incidents**> **Associate.**
  - The **Create Incident** button can also be used to link the call to an open incident. Click on **Create Incident**. A list of incident records appears. Select and open an existing incident record. On the incident form, click the **Link** button. The call is now linked to the open incident.
  - Inform the caller of the incident resolution details (could be a work-around).
  - End the call.
- No - The call is a *new* incident. For field-level information, see *Table 5: New incident--Incident Details tab (apm.quick.g)* in the Field-Level Details section of the Application Administration Guide.
  - Use the **Create Incident** button to open a new incident record. When an incident is created from a call (cc.incquick.g), the call details will automatically populate the contact and incident details tabs for the incident.
  - Validate the category and populate remaining fields.
  - Establish severity. Severity measures the impact of the incident on the business.
  - Assign the incident. For information on assignment groups see *Assignment Groups* on page 41.
- Proceed to *Phase 4: Diagnose Incidents* on page 53.

Initial Analysis Workflow (Phase 3)

```
        ┌─────────────┐
        │  Phase 2    │
        │  Log Call - │
        │  New Call   │
        └─────────────┘
              │
              ▼
     ┌─────────────────┐
     │ Help Desk tries 1st │
     │ level diagnosis │
     │ within set time │
     │ scales          │
     └─────────────────┘
```

```
Problem solved?  ──yes──►  Provide user with solution  ──►  Validate & update call categories  ──►  Mark solution as candidate for Knowledge Base, and update call log  ──►  Close call
     │
     no
     ▼
Set call back flag and issue call number
     │
     ▼
Is call related to an "open" incident?  ──yes──►  Link call to existing incident  ──►  Inform caller of incident resolution details  ──►  (Close call)
     │
     no
     ▼
Open new incident record and validate category type
     │
     ▼
Populate remaining incident fields
     │
     ▼
Establish change severity and inform user
     │
     ▼
Assign incident to SDU (incident clock starts)
     │
     ▼
Phase 4
Diagnose Incidents
```

Phase 4: Diagnose Incidents

1 Assignment group retrieves the next incident

2 Is the incident within the scope of the group's expertise?

- No - One group cannot re-assign an incident to another group. To change the assignment there are two options:
  - Discuss with another group whether they can own the incident. The new group can then assign the incident to themselves.
  - Pass the incident back to the help desk with a recommendation if possible.
- Yes - Assignment group accepts the incident.
  - Acceptance of the incident is signified by changing the incident status to **Work in Progress**.

3 Group attempts to solve the incident

4 Is additional caller info/input required?

- No - proceed to step 5.
- Yes - Attempt to contact the user for additional information
  - Monitor progress to ensure that the response is within set time scales
  - If no contact is made, re-assign the incident to the help desk and suspend the incident clock. Monitoring suspended incidents is a function of the help desk.
  - Help desk then awaits the call from user for further information.
  - Re-start the incident clock when user input is received.

5 Is a permanent solution available?

- Yes - Proceed to *Phase 5: Resolve Open Incidents* on page 55.
- No - Is a a temporary fix available?
  - Yes - Proceed to *Phase 5: Resolve Open Incidents* on page 55.
  - No - determine if another group can provide a fix. If group cannot determine this, re-assign the incident to the help desk.

Diagnose Incidents Workflow (Phase 4)

Phase 3
Initial
Analysis

Assignment group
retrieves problem

Is scope within
group's
expertise? — no → Contact help desk to reassign problem to a new group

yes

Group attempts to
diagnose problem

Is additional
user input/
information
needed? — no → Is a permanent solution available? — no → Is a temporary solution available? — no → Could fix be provided by another group? — no → Notify Service Manager and escalate

yes — (Could fix be provided by another group?) → yes

yes

Attempt to contact
user

yes (permanent) → Phase 5 Resolve Open Incidents ← yes (temporary)

Was contact
made? — no → Reassign incident to help desk → Help desk suspends clock & awaits user call for further information

yes → User input/ information received (restart clock)

Phase 5: Resolve Open Incidents

1 If there is a permanent solution available:

- Provide and test the solution.

- Update the log and change the status to "resolved".

Note: **Closure Code** is a required field. The closure code should reflect the incident's resolution. The out-of-box closure codes are:

- *Advice & Guidance*—The incident was resolved by providing the user with advice and guidance.

- *Fault*—Resolution was provided on a fault that occurred to a system either by the user support assistance, by support staff using remote support tools or by a technician attending the fault location.

- *No Fault Found*—Symptoms of the incident could not be reproduced or replicated either by support staff or the user.

- *User Error*—The incident was caused by accidental damage or inappropriate use of a system.

- *User Closure*—User either solved the incident or the symptoms disappeared between the original call and the attendance of support staff. The user requested that the call be closed.

- *Out of Scope*—This closure code is used for calls that are outside the scope of the support service.

- *Entitlement Failure*—User is unable to provide adequate entitlement details. The call is rejected.

- *Authentication Failure*—User is unable to provide adequate verification of identity when requesting a password to be reset. Reject the call.

- *Temporary Fix*—The incident has been resolved with a temporary fix. A permanent fix is subject to an RFC

Note: This does not account for temporary hardware replacements. In this case, suspend the incident clock after the replacement hardware is provided and the user is operational. When the original hardware is restored, change the incident to "resolved" and close.

- Stop the incident clock.

2 Is there is a permanent or temporary fix available?

- Temporary - Provide and test the temporary fix. The resolution's Closure Code is "temporary fix".

- Permanent - Provide and test the resolution.

  - Flag the resolution as a candidate for the knowledge base.

3 Permanent fixes reflect the ITIL process for Root Cause Analysis:

- Review all temporary fixes.

- Investigate any underlying incidents.

- Generate RFCs or new incident reports to address the underlying incidents.

Resolve Open Incidents Workflow (Phase 5)

```
                    ┌─────────────┐
                    │   Phase 4   │◄──────────┐
                    │  Diagnose   │           │
                    │  Incidents  │           │
                    └─────────────┘           │
                          │               no  │
                          ▼                    │
                       ◇───────◇               │
                      ◇  Solution ◇────────────┘
                      ◇ available? ◇
                       ◇───────◇
                          │
                         yes
                          ▼
                    ◇─────────────◇
                   ◇ Permanent or  ◇   temporary   ┌──────────────┐
                   ◇  temporary    ◇──────────────►│   Provide    │
                   ◇  solution?    ◇               │  temporary   │
                    ◇─────────────◇                │ solution and │
                          │                        │test resolution│
                      permanent                    └──────────────┘
                          ▼
                  ┌──────────────┐
                  │   Provide    │
                  │  permanent   │
                  │ solution and │
                  │test resolution│
                  └──────────────┘
                          │
                          ▼
                  ┌──────────────┐
                  │Flag as candidate│
                  │ for Knowledge │
                  │  Database if  │
                  │   required    │
                  └──────────────┘
                          │
                          ▼
                  ┌──────────────┐
                  │ Update log,   │
                  │change status to│
                  │  "resolved"   │
                  │(Incident clock│
                  │    stops)     │
                  └──────────────┘
                          │
                          ▼
                  ┌──────────────┐
                  │   Phase 6    │
                  │  Validate w/ │
                  │     User     │
                  └──────────────┘
```
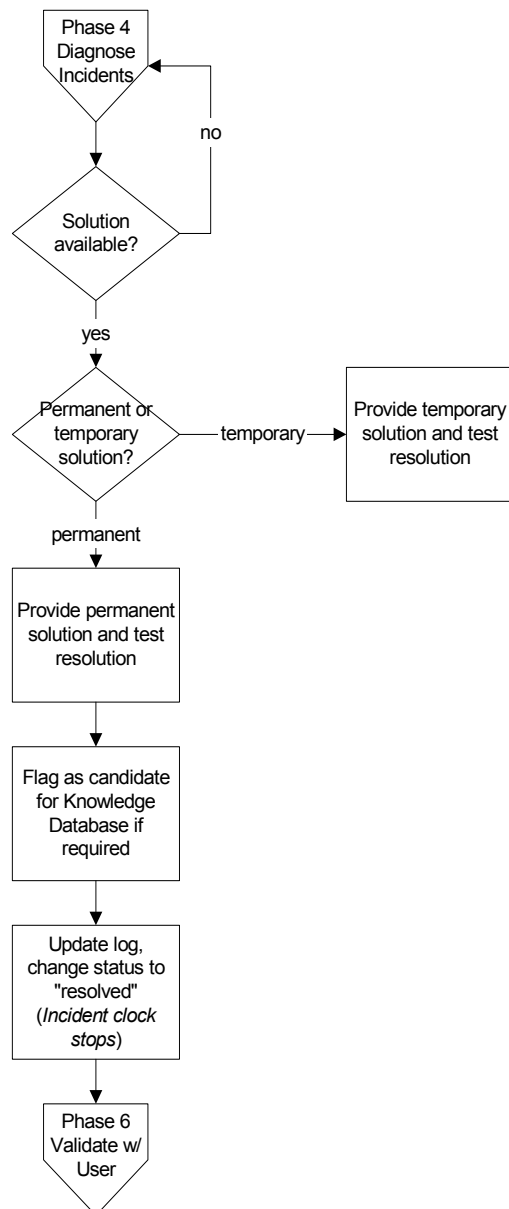
Phase 6: Validate with User

1 Monitor resolved incidents and review linked calls.

2 Is user call back is required?

- No - Close call and notify the user (can be via email).

  Note: In many cases, the system automatically closes the call.

  - Upon incident resolution, it is re-assigned to the help desk.
  - End process.

- Yes - Contact the user to agree on the incident's resolution.

  - If the user required call back, contact the user by the agreed upon method.

3 Able to contact the user?

- No - Attempt to notify via alternate means (fax or email).

  - Monitor user call-back response.
  - Send a final notification to the user.
  - End process.

- Yes - Notify the user that the incident is resolved.

4 Does the user agree that the resolution solved the incident?

- Yes - Close the call with the correct closure code.

  - End process.

- No - investigate the issue.

5 Is the user experiencing the *same* problem?

- No - Validate the user's entitlement and open a new call record.

  - Start at *Phase 1: Receive Call* on page 43.

- Yes - Do you agree with the user?

  - Yes - reopen the incident log and notify the assignment group that the incident remains open.
  - No - Notify the help desk manager. This escalates the incident.

Validate with User Workflow (Phase 6)

```
            ┌─────────────┐
            │  Phase 5    │
            │  Resolve    │
            │  open       │
            │  incidents  │
            └──────┬──────┘
                   │
                   ▼
          ┌──────────────────┐
          │ Monitor resolved │
          │ incidents &review│
          │ linked calls     │
          └────────┬─────────┘
                   │
                   ▼
              ◇ Is call back ◇──no──▶ ┌──────────────┐        ⬭
                 required?            │Close call log│──────▶  End
                   │                 └──────────────┘
                  yes
                   ▼
          ┌──────────────────┐
          │ Contact user to  │
          │ agree closure    │
          └────────┬─────────┘
                   │
                   ▼
              ◇   User   ◇──no──▶┌──────────────┐   ┌───────────────┐   ┌──────────────┐
                contacted?       │User unavailable,│ │Monitor user call│ │Send final    │
                   │             │attemp to notify │ │back response    │ │notification to│
                  yes            └──────────────┘   └───────────────┘   │user          │
                   ▼                                                    └──────────────┘
              ◇Call resolved?◇──yes──▶┌──────────────┐      ⬭
                   │                  │Close call log│──▶  End
                   no                 └──────────────┘
                   ▼
              ◇Same call?◇──no──▶┌──────────────────┐   ┌──────────┐
                   │             │Validate user     │   │ Phase 1  │
                  yes            │entitlement & open│──▶│ Receive  │
                   ▼             │new call record   │   │ call     │
              ◇Agree with◇──no──▶┌──────────────┐     ⬭
                  user?          │Notify assignment│  End
                   │             │group & escalate │
                  yes            └──────────────┘
                   ▼
          ┌──────────────────┐
          │Reopen incident   │
          │log and notify SDU│
          └────────┬─────────┘
                   │
                   ▼
            ┌─────────────┐
            │  Phase 4    │
            │  Diagnose   │
            │  incidents  │
            └─────────────┘
```

3 Root Cause Analysis

CHAPTER

Root cause analysis helps you to identify the underlying, or *root*, cause of a problem or incident, and initiate steps to correct that root cause with a permanent solution. When the underlying problem, or root cause, has been found, a known error record is opened to document the solution for future use. Known errors are then used to initiate the Change Management process. This chapter describes Service Center's Root Cause Analysis (RCA) module.

Topics in this chapter include:

Introduction

Root Cause Analysis (RCA) implements ITIL's Problem Management to find permanent solutions for underlying problems that cause incidents. It also helps minimize the adverse impact of incidents in the IT infrastructure by identifying the root cause.

- When an incident ticket is created, the help desk operator can check the database for known error tickets or find out if the problem matches one already recorded in the Root Cause Analysis (RCA) database. If no match is found, a new root cause analysis record can be opened.

- As the support team works to assess the cause, RCA is used to track the root cause record for future searches. The team implements the solution and notifies the original caller.

- Root cause analysis records can be opened and updated. Reminders can be set for automatic notification for follow-up. Related incident records can be associated with the root cause record, as well as change requests.

- If a work-around solution is found, the root cause ticket can be changed to a known error, accessible through database searches by the help desk staff when creating new incident tickets.

- When a solution has been identified, the known error record is closed. Part of the solution may include improvements to documentation, training, and support procedures.

- As in other modules, tickets are automatically sent to the inboxes of appropriate personnel and managers. Extensive searches of the database and knowledge base support the investigation, tracking, and resolution of the underlying problems.

For further details of using and setting up Root Cause Analysis, see the *User's Guide* and the *Application Administration Guide*.

The goals of Root Cause Analysis (RCA)

The purpose of Root Cause Analysis is to:

- Find errors in the IT infrastructure, record them, track their history, find resolutions for them, and prevent their recurrence.

- Record resolutions so that they are quickly and easily available to support, training, and documentation personnel.

- Find needs for improvements in training or documentation, and make the data to fix them easily accessible.
- Reactively resolve problems related to incidents.
- Proactively resolve problems before incidents occur.

RCA links with both Incident Management and Change Management.

Root Cause Analysis (RCA) and Incident Management

The main goal of Incident Management is to get the client up and running quickly. This is often done through a work-around, rather than through a permanent solution.

The main goal of RCA is to find the underlying cause and a *permanent solution* that will prevent future incidents. This takes more time initially, but causes service to improve in the long run.

Root Cause Analysis is related to Incident Management in several ways.

- Root Cause tickets can be opened from incident tickets.
- Details and histories included in incident records are used for analysis purposes. RCA cannot function effectively without those details.
- Incident records are linked to RCA records.
- The knowledge base that is built and maintained in RCA supplies solutions for incident tickets.

How Root Cause Analysis works

Root Cause Analysis allows you to automatically view related incidents and known error records. You can select and open these dependent records directly from the list view.

Root cause tickets are for informational purposes only. The appropriate personnel can escalate and reassign root cause tickets. The system can also automatically issue alerts and escalate a root cause that is not getting resolved.

Root cause tickets can be:

- Opened for any incident reported.
- Sent automatically to the proper system personnel.
- Tracked and resolved by the personnel and system managers.
- Sent by e-mail or fax to the user with a resolution to the reported root cause.

Root Cause Analysis Process Flow

Root Cause Analysis

```
[Service Desk Call] → <Incident immediately resolved?> —Yes→ (Resolve incident)
                              │
                              No
                              ↓
                      [Create Incident ticket]
                              ↓
[Give workaround to customer] ←Yes— <Match in Known Error database?>
           │                              │
           ↓                              No
[Update incident record                   ↓
 with Known Error ID]            <Match in RCA database?> —Yes→ [Update incident record with RCA ID]
           │                              │                              │
           ↓                              No                             ↓
[Update incident record                   ↓                   [Update incident record
 with Classification Data]                │                    with Classification Data]
           │                              │                              │
           ↓                              ↓                              ↓
[Update Known Error            [Open new RCA]              [Update RCA record
 record with incident count]        │                      with incident count]
           │                        ↓                              │
           ↓              [RCA team works on solution]            ↓
[Check for problem                  ↑                   [Check for problem
 resolution in Known          Yes   │   Yes              resolution in RCA
 Error database.]                                        database.]
           │                        ↓                              │
           ↓              [Add solution to                         ↓
<Is further work          Known Error or RCA]        <Is further work required?>
 required?>                         │
           No                       ↓                     No
           └──────→      (Implement solution)  ←──────────┘

(Give workaround or solution to customer) ← loop back
```

Root Cause Analysis Activities

RCA best practice activities are an important aspect of your infrastructure's stability. Having the ability to identify root causes, find permanent solutions, plan for and track changes, and prevent future incidents keeps you on top of your infrastructure.

The main activities within the scope of RCA are:

- Identify and eliminate root causes
- Identify and maintain Known Errors
- Define Structural solutions

Proactive Root Cause Analysis

Proactive RCA is concerned with identifying root causes and resolving problems and known errors before incidents occur. Both problem and error control are reactive; both deal with problems and identify known errors only after an incident has occurred.

These activities can be the prevention of problems or strategic decisions.

- Trend analysis
- Preventive action

Problem Control

Root cause analysis problem control activities help you identify the root cause of incidents and provide relevant information to the help desk. Advice on work-arounds, if applicable, is also given.

Problem control activities
- A problem is identified when:
  - Incident data reveals recurring incidents
  - Incident data shows that incidents are not matched to existing known errors
  - IT infrastructure analysis shows that a problem could lead to incidents
  - A major incident occurs for which a structural fix is needed

Note: Add problem records to the database and link the problem records to all associated Incident records. Also record the solution and/or work-around in the problem record.

- Problem classification:

  Classifying problems helps you determine the impact of a failing component as well as the amount of effort required to recover that component.

  - Determine: category, impact, urgency, and priority.
  - Urgency can be influenced by: availability of a temporary fix or a work-around, the possibility of planned delay of a resolution, and awareness of impact on business.

Note: Urgency indicates how long a problem can be delayed. Priority indicates the *order* in which problems should be addressed.

- Problem investigation and diagnosis:
  - The goal is to diagnose the underlying cause of known errors.
  - Investigation includes available work-arounds for incidents related to the problem.
  - Problem records are updated with recommended work- arounds.

Error Control

The error control process begins upon the detection of an underlying problem. Error control activities focus on processing known errors until they are eliminated by the implementation of a change.

Error control activities

- Error identification and recording
  - An error is identified when a Problem is detected.
  - The error becomes a *known error* when the root cause of the problem is found and a work-around is provided.
  - Make sure that the root cause ticket is updated with all resolution activity.

- Error assessment
  - Perform an initial assessment of the means of resolving the error.
  - If necessary, complete a request for change.
  - Link the request for change record to the known error record.
- Error resolution recording
  - Record the resolution for known errors in the root cause analysis system.
  - Enter data into the knowledge base. This base holds data on configuration items, symptoms, and resolutions. This way, the data is available for help with future incidents and known errors.
- Error closure
  - Close the known error record after changes have been successfully implemented.
  - Close any associated incident or root cause tickets.
- Problem/error resolution monitoring
  - Error control monitors progress in resolving known errors; Change Management is responsible for the processing of request for changes.
  - Root cause analysis monitors the impact of problems and known errors on services.
  - If the impact becomes severe, root cause analysis escalates the problem.

4 Change Management

CHAPTER

Change management is the process of identifying a future desired state for the business, understanding the current state, and constructing a transition plan that describes the steps required to attain the goal.

This chapter describes how to use Change management to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to an organization's infrastructure.

Topics in this chapter include:

Introduction

The goal of Change Management (CM) is to minimize the impact of changes on the quality of service. Typically, a change has been identified as part of the resolution of incident tickets or for resolving root cause records and known errors. Changes such as upgrades to central servers or network installations often impact several users.

By its out-of-box workflow, Change Management enables personnel and management to:

- Create a request for change (RFC) ticket, assigning a unique number against which all activity can be tracked and reported. Changes are classified by categories, including default categories such as HW (hardware), and MAC (general purpose move/add/change). Site-specific categories can also be defined.

- Within a change record, identify the tasks (work processes) required to accomplish the change. The system can automatically notify those responsible for accomplishing the tasks. Inboxes provide a convenient way for technicians to manage their workload. Tasks are also assigned categories to facilitate tracking, reporting, and assignment.

- Follow, track, and query on a standard workflow through the entire implementation cycle. Phases are groupings of activities within a task or change that identify the logical sequence of repeatable steps within the change implementation cycle. Typically, an RFC might have four phases:

  - Assessment phase - for opening and approving the RFC.

  - Building phase - for assigning the person who is actually implementing the change.

  - Testing phase - for recording the test data and the testing results for the change. If the test fails, the phase automatically reverts back to the Build phase.

  - Implementation phase - assuming success in testing, the change can be implemented. Details of the implementation can be recorded, including a review process that documents the success or failure of the change.

For further details about using and setting up Change Management, see the *User's Guide* and the *Application Administration Guide*.

ServiceCenter out-of-box workflow enables you to:

- Put the help desk in control and ensure that poorly planned changes do not effect the business.
- Calculate both business and operational risk.
- Associate calls to incidents, incidents to known errors, and manages the resolution process.
- Notify change approvers in order of authority when an RFC is created.
- Automatically notify users of completions and deadlines.

Phase 1: Record	→	Phase 2: Assess	→	Phase 3: Plan	→	Phase 4: Build	→	Phase 5: Implement	→	Phase 6: Accept/ Close
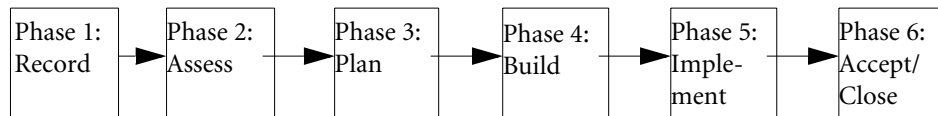
Scope

ServiceCenter out-of-box workflow guides you through the basic Change Management activities, from planning for changes to the implementation of changes to your infrastructure.

- **Change logging**

  Follow procedures for documenting RFCs. Decide which members of your organization should be authorized to *request* changes.

- **Allocation of priorities**

  Every RFC must be assigned a priority. The priority is base on both the impact of a problem and its urgency.

- **Change categorization**

  Consider the amount of risk associated with each RFC before giving final approval to the change. Decide how to proceed based on the category that the RFC is assigned.

- **Impact & Resource assessment**

  Consider:

  - - The impact the change will have on business operations
  - - The effect the change will have on the infrastructure
  - - The impact on other services in the infrastructure
  - - The effect of *not* implementing the change
  - - The IT and other resources that are needed to implement the change

- **Change approval**

  Decide on the levels of change approval and which members of your organization will be authorized to approve changes

- **Change scheduling**

  Is it more practical to implement one change at a time or numerous changes at the same time? Schedule changes to have the least amount of impact on normal business operations.

- **Change building testing & implementation**

  Implement and test the change.

- **Change review**

  Review all implemented changes after a pre-determined amount of time has elapsed. Check that the change had the desired effect, users are content with the change, and that the change was implemented on time and at cost.

Requests for Change (RFC)

Best practices specify that changes to the infrastructure should always be driven by a formal RFC. When an RFC has been received and the business requirements and current state are understood the change process can be started.

Once a call has been received, entitlement has been checked, and the call has been identified as an RFC call, the call is routed to Change Management.

First, a project plan is drafted. Required resources are identified and a back out or contingency plan is created. Next, an impact analysis of the RFC is carried out and the level of risk is determined. Finally, the plan is tested, implementation begins, approved changes are tracked at key milestones, and a post project assessment is performed.

Note: Before the change process can be started it is necessary to understand the current state of the infrastructure, all related systems, and how those systems are used by the business.

RFCs refer to requirements to change elements of the IT infrastructure such as:

- Procurement and installation of new equipment
- System upgrades
- Office moves
- Operating system or application upgrades
- Installation of new software
- Installation of IT equipment into a new building

All such requests are subject to the request for change process.

Categorizing Requests

There are two reasons for categorizing request for change.

- To determine what level of change is inclusive of the IT service charge, and what will incur additional cost.
- To ensure that all requested changes that carry significant risk to business are controlled and implemented to minimize such risk.

RFC Categories

RFCs are categorized as follows:

Category 1 - Major Business Change—Request for a large-scale change to business platform, operating system, business unit location move, add new business or major location to service

Category 2 - Business Change—Request for distributed software upgrade such as a new anti-virus version, move of business unit to a different area of same location, or a change to standard configuration

Category 3 - Minor Change—Request to install or move up to 10 new workstations or associated assets including software of standard configuration within a single location

Change priorities

The change priorities are as follows:

Emergency Changes—An emergency change exists for the sole purpose of implementing a critical modification to a live environment, while preventing interruption to business activities. The life cycle is followed retrospectively for an emergency change and requires the highest level of authorization.

Expedited Change—An expedited change is made when a business reason requires implementation of the change in a shorter time scale than that contained within the Service Level Agreement. Expedited changes follow an accelerated form of the complete change life cycle, and thus requires an increased level of authorization.

Normal Change—A normal change is made within the time scale defined in the Service Level Agreement.

Change category definitions

IMAC—Procurement, installation, move, change or upgrade involving a single engineer visit to a user's desk to complete the requested service, incorporating directly connected peripherals. Standard IMACS are those that strictly adhere to the SLA in terms of numbers involved, service time scales, low business risk, and agreed configurations.

User Administration—Adding, deleting or changing user access profiles to systems such as shared servers, email, business applications and databases. Where practical, such operations would be carried out from the service desk using remote or enterprise management tools in accordance with the client's security policies and guidelines.

Procurement only—Where no installation or configuration activity is required by a user such as for a PDA or mobile phone. This change ensures that the item is recorded on the asset database.

Network—Change involving the data communications infrastructure subdivided into 3 types with different default impact categories.

Telecoms—Configuration change required for the voice infrastructure.

Business Applications—Change to business application code involving the distribution of software to client systems or distributed servers or the introduction of a software change to a host system.

Shared Infrastructure—Change to the hardware, operating system, or location of an item of shared infrastructure, other than the communication network. This reflects the nature of the system to be changed and therefore its corresponding default impact category.

Security—Change to security policy or protection mechanism. This would include the updating of anti-virus software or a change to "after hours" access to client premises.

Service Management—Change to the contractual requirements of the service such as the introduction of a new client site.

Training—Request for training for individual or group of users.

Facilities—Change requested for client site facilities such as the move of office furniture.

Other—Change that does not meet the definitions of the above change types. These will be reviewed to ensure the correct type is assigned or that other change types should be introduced.

Change status

The change process is sub-divided into 6 phases: record, assess, plan, build, implement, and accept/close. Each of these phases is managed using the following status flags:

Initial Pending—Awaiting acceptance of the request for change into the phase.

Initial Approved—The request for change has been accepted and is currently passing through the phase.

Initial Disapproved—The request for change has not been accepted into the phase. This means that it has failed the relevant approval task and has therefore been rejected. In all such cases the request for change will be closed, and a new request for change can be created as required.

Closed Approval—The request for change has successfully completed the phase. This status change will also start the following phase at the "Initial Pending" status.

Closed Disapproved—The request for change has failed to complete the phase and has been rejected. In all such cases the request for change will be closed, and a new request for change can be created as required.

Phase & Change Closure Codes

Completed—Change has been successfully completed and accepted by the user. All associated administration, such as informing the asset database administrator, has also been completed.

Failed—Change failed during implementation and regressed to an agreed previous state. No further action to be undertaken on this change.

Rejected-Financial—The client rejects the change during the process for financial reasons.

Rejected-Technical—The change is rejected because it can not be technically achieved within the standards, guidelines and strategies agreed with the client.

Rejected-Security—The change is rejected because it would compromise the client's security policy, such as an employee request for access rights to the personnel system.

Withdrawn—Change is withdrawn by the initiator of the request prior to reaching formal authorization points.

Change Management roles

The following terms are used throughout this chapter to identify the various roles in Change Management.

Change Administrator— The Change Management Administrator.

Change Initiator—A person who may not have the authority to request a change and therefore works through a Change Sponsor.

Change Owner—The coordinator and person responsible for getting the entire change completed.

Change Sponsor—Person who has the authority to request a change, either for them self or another person or group.

Change Management workflow

Phase 1: Record

1 Complete request for change details and determine category

- All updates to free-form test in the Call record will be pasted into the Change record when the request for change is created. In addition, the contact details are pasted into the request for change contact tab.

- The details for the Change Initiator and any relevant asset are already collected.

- Select a Change Sponsor from the table of Change Sponsors.

2 Ensure all details are complete

- If the request for change has been submitted electronically, call the Change Initiator.

3 Assign Change Owner

- This role is pre-defined from the request for change type.

4 Inform the Change Initiator of the request for change reference number

- This is the request for change number. The caller is not given the call number. Updates are made to the request for change description tab.

Record Workflow

```
                    ┌─────────────┐
                    │    Start    │
                    └─────────────┘
                           │
                           ▼
              ┌─────────────────────────┐
              │    Change Initiator     │
              │   completes request     │
              │   for change form       │
              │   and sends request     │
              │      to Change          │
              │    Administration       │
              └─────────────────────────┘
                           │
                           ▼
              ┌─────────────────────────┐
              │   Complete request      │
              │  for change details;    │
              │      determine          │◄──────────────┐
              │   category and          │               │
              │   select a Change       │               │
              │      Sponsor            │               │
              └─────────────────────────┘               │
                           │                            │
                           ▼                   ┌──────────────────┐
                      ╱─────────╲              │  Contact Change   │
                     ╱ Are all   ╲    no       │ Initiator and obtain │
                    ╱  details    ╲───────────►│   the required    │
                    ╲  complete?  ╱             │     details       │
                     ╲           ╱              └──────────────────┘
                      ╲─────────╱
                           │
                          yes
                           ▼
              ┌─────────────────────────┐
              │   Change Sponsor        │
              │   allocates a           │
              │   Change Owner          │
              └─────────────────────────┘
                           │
                           ▼
              ┌─────────────────────────┐
              │   Change Owner          │
              │   informs Change        │
              │   Initiator of the      │
              │   request for change    │
              │   reference number      │
              └─────────────────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │   Phase 2   │
                    │   Assess    │
                    └──────┬──────┘
                           ▽
```
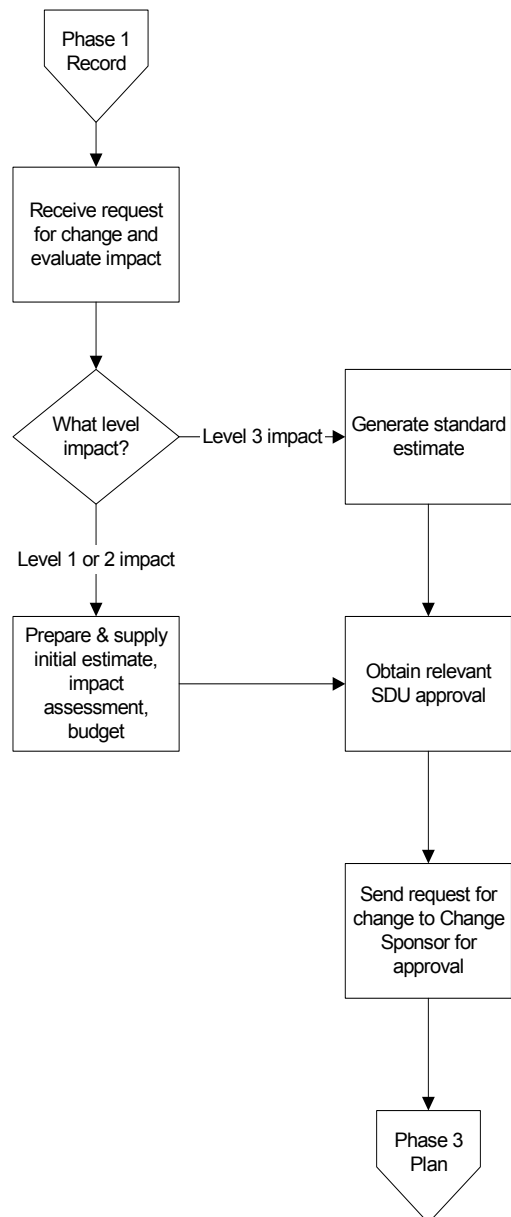
Phase 2: Assess

1 Receive request for change, validate impact and confirm priority

   ■ If the priority is changed to Expedited or Emergency, the request for change is accelerated through the ServiceCenter system.

2 Generate standard estimate

   ■ Each project should publish rules covering the price, cost and implementation plan.

3 Prepare and supply initial estimate, initial impact assessment, budget

4 Change Administrator sends estimate for approval by Change Sponsor

5 Obtain service desk approval

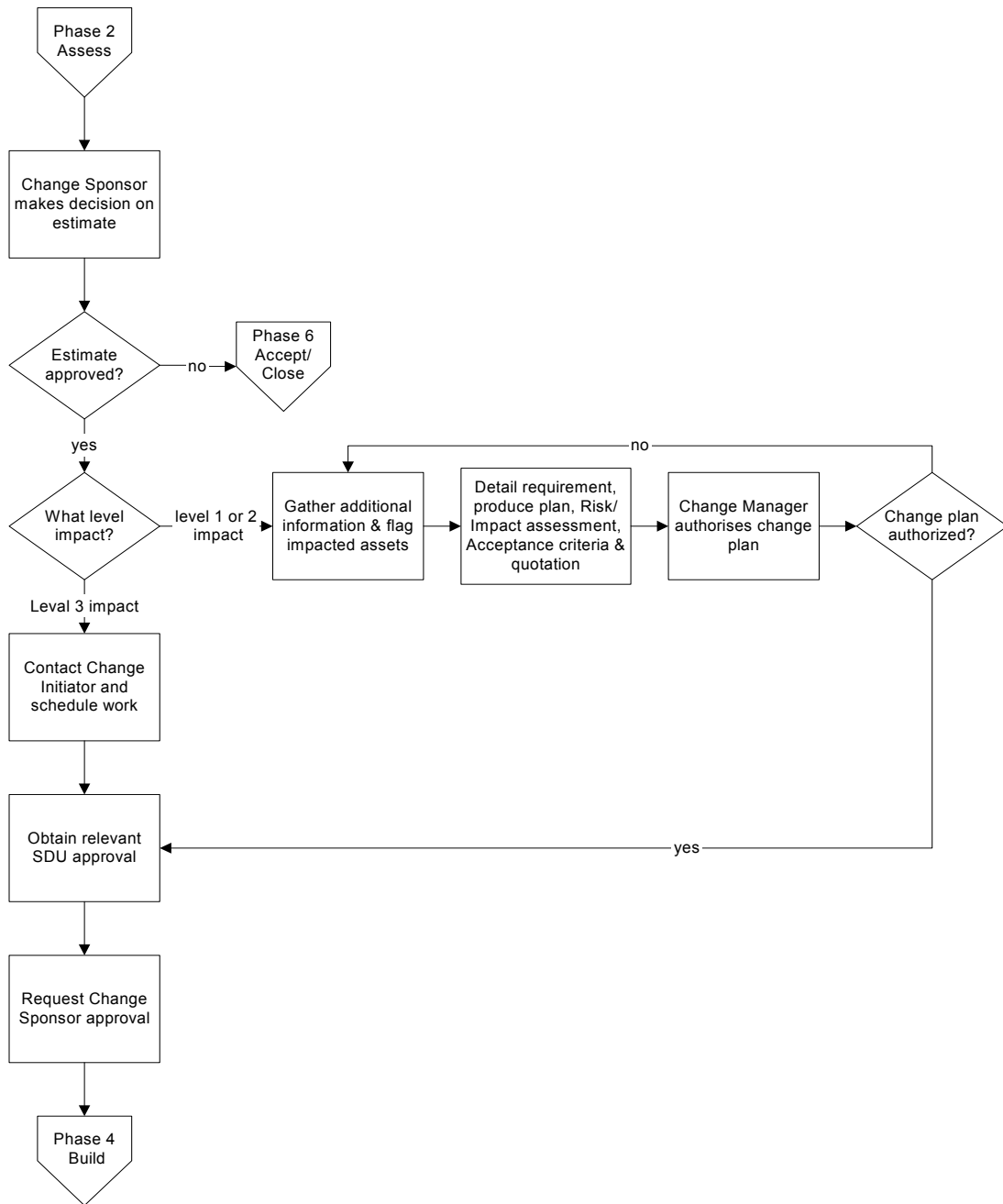   ■ The purpose is to enable commitment of effort, prevention of errors, and the scheduling of resources.

Assess Workflow

```
        ┌──────────────┐
        │  Phase 1     │
        │  Record      │
        └──────┬───────┘
               │
               ▼
     ┌──────────────────┐
     │ Receive request  │
     │ for change and   │
     │ evaluate impact  │
     └────────┬─────────┘
              │
              ▼
         ◇ What level ◇ ──── Level 3 impact ──▶ ┌──────────────────┐
         ◇  impact?   ◇                          │ Generate standard│
         ◇            ◇                          │ estimate         │
                                                 └────────┬─────────┘
              │                                           │
      Level 1 or 2 impact                                 │
              │                                           ▼
     ┌──────────────────┐                      ┌──────────────────┐
     │ Prepare & supply │                      │ Obtain relevant  │
     │ initial estimate,│ ───────────────────▶ │ SDU approval     │
     │ impact           │                      │                  │
     │ assessment,      │                      └────────┬─────────┘
     │ budget           │                               │
     └──────────────────┘                               ▼
                                            ┌──────────────────┐
                                            │ Send request for │
                                            │ change to Change │
                                            │ Sponsor for      │
                                            │ approval         │
                                            └────────┬─────────┘
                                                     │
                                                     ▼
                                              ┌────────────┐
                                              │ Phase 3    │
                                              │ Plan       │
                                              └────────────┘
```

Phase 3: Plan

1 Sponsor makes decision on estimate

- Notify the Change Sponsor by email of the need for approval. There is a field for the Change Sponsor to add comments.
- Suspend the clock while you wait for approval.
- A request for change can be Approved or Disapproved.
- Disapproval leads to closure of the request for change. Disapproval due to the wrong change sponsor being assigned the request for change also closes the request for change. Then, the Change Initiator nominates a new change sponsor.

2 Contact initiator and schedule work

- Level 3 impact request for change must have pre-defined plans, regression rules and acceptance criteria that are produced by implementation projects.
- Some request for change are standard enough that the whole Plan and Build phases are pre-determined and do not require further approval.

3 Gather additional information, and flag affected assets

- The Change Owner is in a position to flag accepted assets. The rules for flagging are dependent on the individual contracts.
- The Change Owner flags the asset tags within the request for change.

4 Detail requirement, produce plan, acceptance, impact assessment and quotation

- All of the above elements are required, dependent on the nature of the request for change.

5 Authorize plan

- The Change Manager checks the plan for quality and completeness and if necessary rejects it for additional information to be supplied.

Plan Workflow

```
        Phase 2
        Assess
           │
           ▼
    ┌──────────────┐
    │ Change Sponsor│
    │ makes decision on│
    │   estimate    │
    └──────────────┘
           │
           ▼
       Estimate ──── no ───►  Phase 6
       approved?              Accept/
           │                   Close
          yes
           │
           ▼
      What level ── level 1 or 2 ──►┌──────────────┐   ┌──────────────┐   ┌──────────────┐      Change plan
       impact?        impact        │Gather additional│  │Detail requirement,│ │Change Manager│     authorized?
           │                        │information & flag│─►│produce plan, Risk/│─►│authorises change│─►
    Level 3 impact                  │impacted assets │  │Impact assessment,│  │    plan     │
           │                        └──────────────┘   │Acceptance criteria &│ └──────────────┘
           ▼                                            │   quotation   │
    ┌──────────────┐                                    └──────────────┘
    │Contact Change│
    │ Initiator and│
    │ schedule work│
    └──────────────┘
           │
           ▼
    ┌──────────────┐
    │Obtain relevant│ ◄──────────── yes ────────────
    │ SDU approval │
    └──────────────┘
           │
           ▼
    ┌──────────────┐
    │Request Change│
    │Sponsor approval│
    └──────────────┘
           │
           ▼
        Phase 4
        Build
```

Phase 4: Build

1 Sponsor makes decision on plan

- Notify the Change Sponsor of the need for approval
- Suspend the clock while you wait for approval
- Upon formal disapproval of the plan, close the request for change. However, minor changes can be made upon agreement between the Change Sponsor and the Change Owner without formally disapproving the plan.
- Disapproval due to rejection of the approach or requirement changes also results in closure of the request for change and the creation of a new one. Re-use applicable material from the disapproved request for change and expedite the new request for change.

2 Assign to change owner

- In some cases, the request for change may need to be re-assigned to a new Change Owner.

3 Assign all build tasks

- The Change Owner assigns the build tasks in line with the plan. Each task has a Task Owner.
- ServiceCenter has the concept of tasks which can be assigned within a phase and which must all be completed before progress to the next phase.

4 Produce regression plan

- This plan is usually produced over time.

Build Workflow

```
                          ┌─────────────┐
                          │  Phase 3    │
                          │  Plan       │
                          └──────┬──────┘
                                 │
                                 ▼
                          ┌─────────────┐
                          │Change Sponsor│
                          │makes decision│
                          │on request for│
                          │   change    │
                          └──────┬──────┘
                                 │
                                 ▼
                          ◇ Is request ◇        ┌─────────┐
                          ◇ for change  ◇──no──▶│ Phase 6 │
                          ◇ approved?   ◇        │ Accept/ │
                          ◇            ◇        │ Close   │
                                 │              └─────────┘
                                yes
                                 ▼
                          ┌─────────────┐
                          │   Change    │
                          │Administrator│
                          │assigns request│
                          │for change to a│
                          │new Change   │
                          │   Owner     │
                          └──────┬──────┘
                                 │
                                 ▼
                          ┌─────────────┐
                    ┌────▶│ Change Owner│
                    │     │assigns all build│
                    │     │   tasks     │
                    │     └──────┬──────┘
                    │            │
                    │            ▼
                    │     ┌─────────────┐
                    │     │ Build change│
                    │     └──────┬──────┘
                    │            │
                    │            ▼
                    │     ┌─────────────┐
                    │     │Test change  │
                    │     │   build     │
                    │     └──────┬──────┘
                   no            │
                    │            ▼
                    │        ◇Passed?◇──yes──▶ Obtain relevant ──▶ Request ──▶ Phase 5
                    └────────────┘             SDU approval     authorization  Implement
                                                                for
                                                                implementation
```

Phase 5: Implement

1 Change Owner authorizes the implementation

- This task is coordinated between the Change Owner and the Change Initiator.

2 Change Sponsor authorizes the implementation

- The relevant Change Sponsor is notified by email of the need for approval. Approval can be made by logging on and approving.

- The clock is suspended while awaiting approval.

3 Assign all implementation tasks

- There should now be more detail than was available during the build phase.

Implement Workflow

```
        ┌──────────┐
        │ Phase 4  │
        │  Build   │
        └────┬─────┘
             │
             ▼
   ┌───────────────────┐
   │ Change Sponsor,   │
   │ Change Owner      │
   │ authorize change  │
   │ build             │
   └─────────┬─────────┘
             │
             ▼
        ◇ Build ◇ ── no ──▶  Phase 6
        ◇approved?◇            Accept/
             │                 Close
            yes
             │
             ▼
   ┌───────────────────┐
   │ Assign resources  │ ◀────────────┐
   │ for all           │              │
   │ implementation    │              │
   │ tasks             │              │
   └─────────┬─────────┘              │
             │                        │
             ▼                        │
   ┌───────────────────┐              │
   │ Implement the     │              │
   │ change            │              │
   └─────────┬─────────┘              │
             │                        │
             ▼                        │
   ┌───────────────────┐              │
   │ Monitor change    │              │
   │ implementation    │              │
   │ tasks             │              │
   └─────────┬─────────┘              │
             │                        │
             ▼                        │
   ┌───────────────────┐              │
   │ Test the          │              │
   │ implementation    │              │
   └─────────┬─────────┘              │
             │                        │
             ▼                ┌──────────────┐
      ◇Implementation◇ ─ no ─▶│Regress change│
      ◇ successful? ◇         │and reschedule│
             │                └──────────────┘
            yes
             │
             ▼
        ┌──────────┐
        │ Phase 6  │
        │ Accept/  │
        │  Close   │
        └──────────┘
```
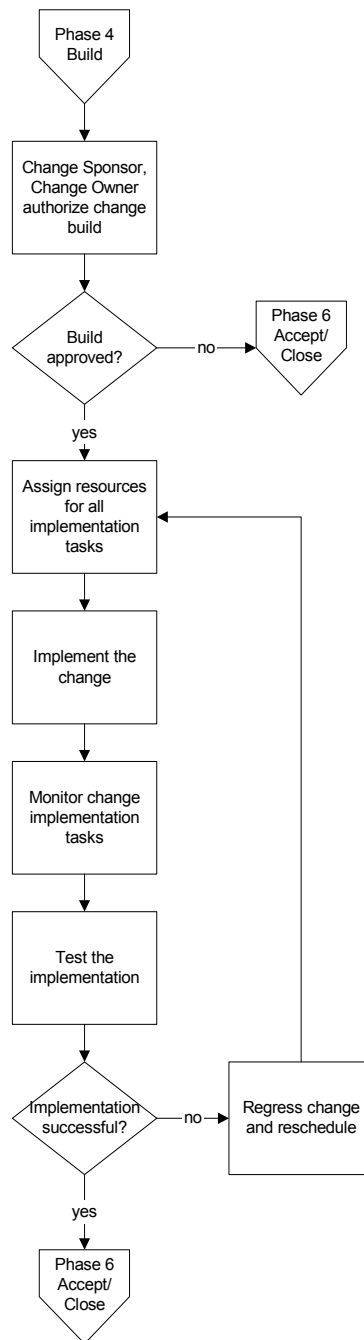
Phase 6: Accept/Close

1 Sign off ready for acceptance

- The level of formality depends on the request for change category and the acceptance criteria for the request for change.
- The clock used for SLA measurements is stopped now.

2 Investigate and regression

- This involves procedures specific to the individual managed service.

3 Close the request for change

- Includes entry of a closure code and marking the solution as a candidate for the knowledge base.

Accept/Close Workflow

```
        Phase 5
        Implement
            │
            ▼
    Sign off ready for
       acceptance
            │
            ▼
      Test change
            │
            ▼
      Change          ── no ──▶  Investigate issue  ──▶  Issue      ── no ──▶  Phase 5
      accepted?                                          resolved?             Implement
            │                                                │
           yes                                              yes
            │                                                │
            ▼                                                │
    Notify Change  ◀──────────────── yes ────────────────────┘
  Initiator of change
        closure
            │
            ▼
    Submit asset
    amendments to
     Inventory &
    Configuration
     Management
            │
            ▼
      Close RFC
            │
            ▼
          End
```
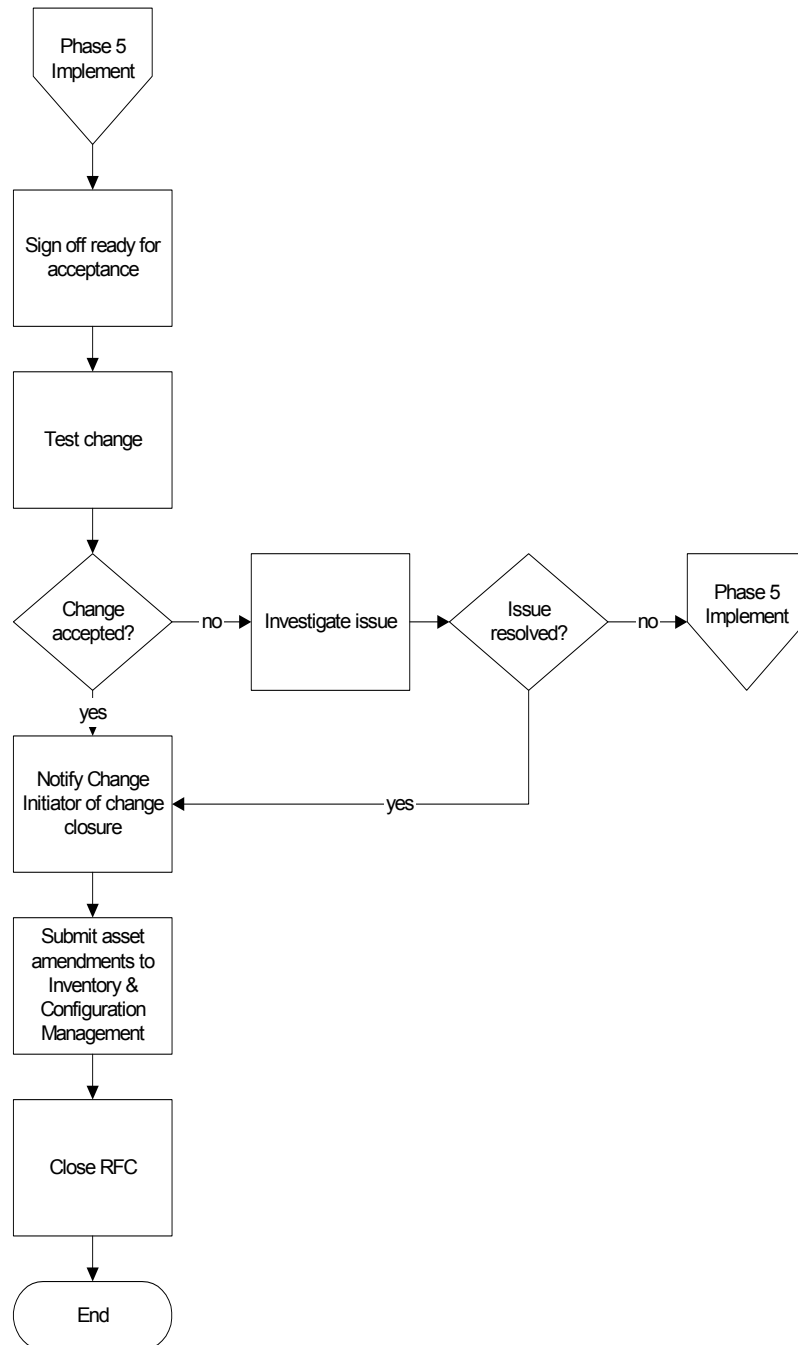
5 Inventory Management

Inventory Management (abbreviated as ICM for Inventory and Configuration Management) enables enterprises to efficiently identify, control, maintain, and verify the versions of configuration items (CIs) that exist in their IT infrastructure.

This chapter describes how to use Inventory Management to help track software and hardware components and their relationships in the network by creating records about devices, service information, and PC software.

Topics in this chapter include:

- *Introduction* on page 92
- *ICM workflow* on page 93

Introduction

Accurate tracking of incidents and changes starts with control of resources and their relationships. Following industry best practices gives you the ability to *plan* for changes, rather than just implement them as they are needed. This is an important part of ICM because planning ahead enables you to understand the impact that an incident or change could have on your infrastructure.

All assets are defined in the device file, the foundation of Inventory Management. For each record, details can include contact, location, vendor, and outage history. Other ServiceCenter applications, such as Incident Management and Change Management, access ICM's repository of data in the inventory files to populate fields on forms through the use of link records.

For further details of using and setting up Inventory Management, see the *User's Guide* and the *Application Administration Guide*.

ServiceCenter's ICM out-of-box workflow tracks the IT assets and configurations that make up the infrastructure. This can be hardware, software and associated documentation. The inter-relationships between these components are also monitored.

ICM forms the foundation for Incident Management, Root Cause Analysis, and Change Management, as detailed in subsequent chapters of this guide.

Scope

There are five basic activities in ICM. Adopting a process that encompasses all five of these activities ensures that assets are tracked and monitored effectively.

The basic activities within the scope of ICM are:

- **Planning**

  Plan the function, scope, and objectives of ICM for your organization.

- **Identification and Data Collection**

  Identify and label all of your company's existing IT components. The information you track includes asset identification, contact, asset network relationship, and model/version data. Enter this information into the database.

- **Inventory Maintenance**

  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 RFC.

- **Reporting**

  Run reports of the current and historical data that is concerned with each IT component throughout its life cycle. Status accounting makes changes to components trackable.

- **Verification and Audit**

  Check and verify physical existence of IT components and ensure that they are correctly recorded in the database.

ICM workflow

Phase 1: Planning	→	Phase 2: Identification and Data Collection	→	Phase 3: Inventory Maintenance	→	Phase 4: Reporting	→	Phase 5: Verification and Audit
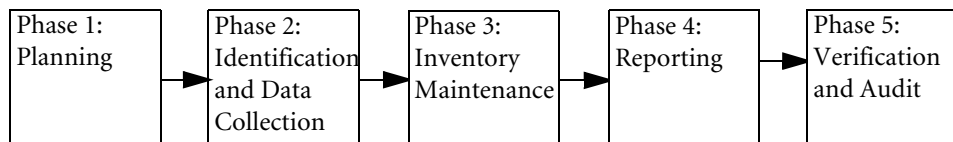
The following steps are based on ITIL standard processes.

Phase 1: Planning

The following steps guide you through the Planning phase.

1 Create a Configuration Management plan for your organization defining the following:

- Configuration Management purpose, scope, and objectives
- Configuration Management roles and responsibilities
- Configuration Items (CI) naming conventions
- the schedule and procedures for performing Configuration Management activities:
  - Planning
  - Identification and Data Collection
  - Inventory Maintenance
  - Reporting
  - Verification and Audit

- Configuration Management systems design, including scope and key interfaces.
- housekeeping, including license management and CI retention period.

2 Regularly review workload and resource performance relative to the plan and correct deficiencies.

3 Compare cost of capturing and keeping CI details with current benefits; purge any unnecessary or redundant data.

Planning Workflow

```
      ┌─────────────┐
     (    Start      )
     (   Phase 1     )
      (  Planning    )
       └──────┬──────┘
              │
              ▼
       ┌─────────────┐
       │             │
       │ Create a CM │
       │    plan     │
       │             │
       └──────┬──────┘
              │
              ▼
       ┌─────────────┐
       │   Review    │
       │ performance │
       │against plan &│
       │   correct   │
       │ deficiencies│
       └──────┬──────┘
              │
              ▼
       ┌─────────────┐
       │Compare CI data│
       │collection benefits│
       │ against costs &│
       │make adjustments│
       └──────┬──────┘
              │
              ▼
       ┌─────────────┐
       │   Phase 2   │
       │Identification and│
        │Data Collection│
         └────┬────┘
              ▼
```
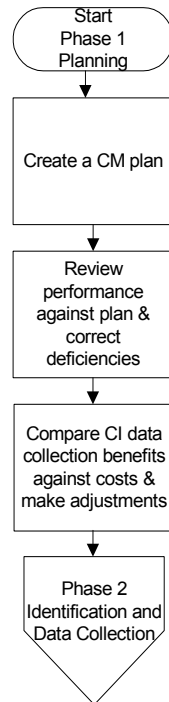
Phase 2: Identification and Data Collection

The following steps guide you through the Identification and Data Collection phase.

1 Take a physical inventory of your IT components and tag them with asset IDs.

If a physical audit is not possible, transfer updated data from existing records.

2 Enter component data into the database.

Enter data into the database for all of your assets, including hardware, network components, system software, custom built applications, and physical databases.

Consider:

- To what level of detail do you require asset data? (For example, What information about personal computers is sufficient? You may require detailed data for assets such as memory, hard disk space, CD-ROM speed, monitors, and keyboards.)
- Are there constraints on the size of your database for storing inventory data?
- Planning Workflow

Identification and Data Collection Workflow

```
        ┌─────────────┐
        │  Phase 1    │
        │  Planning   │
        └──────┬──────┘
               │
               ▼
  ┌──────────────────────┐
  │  Take physical       │
  │  inventory of all IT │
  │  components and      │
  │  assign asset ID     │
  │  tags                │
  └──────────┬───────────┘
             │
             ▼
  ┌──────────────────────┐
  │  Enter component     │
  │  data                │
  └──────────┬───────────┘
             │
             ▼
        ┌─────────────┐
        │  Phase 3    │
        │  Inventory  │
        │ Maintenance │
        └─────────────┘
```
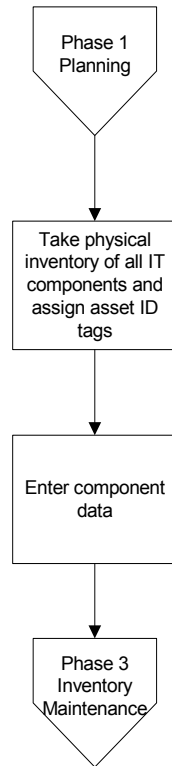
Phase 3: Inventory Maintenance

Periodically performing the steps for inventory maintenance ensures that your infrastructure is stable and that you have control of your assets.

The following steps guide you through the Inventory Maintenance phase.

1 Reconcile and assign software licenses to assets.

- Produce a list of the procured licenses.
- Include the following details: License duration, software version, and the number of installations that the license covers.
- Run a report to find installed software that does not have a license.
- Check the list against registered licenses.
- Reconcile any unlicensed software with available licenses or obtain new licenses.

2 Assign assets to contracts.

3 Review asset assignments.

4 Update asset status values.

5 Archive and purge historical data.

Inventory Maintenance Workflow

```
      ┌─────────────┐
      │  Phase 2    │
      │Identification│
      │  and Data   │
      │ Collection  │
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │ Reconcile and│
      │assign software│
      │licenses to assets│
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │Assign assets to│
      │  contracts  │
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │ Review asset │
      │ assignments │
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │ Update asset │
      │  status and  │
      │administrative│
      │details as required│
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │ Perform all  │
      │archiving and │
      │   storage    │
      └─────────────┘
            │
            ▼
      ┌─────────────┐
      │  Phase 4    │
      │ Reporting   │
      └─────────────┘
```
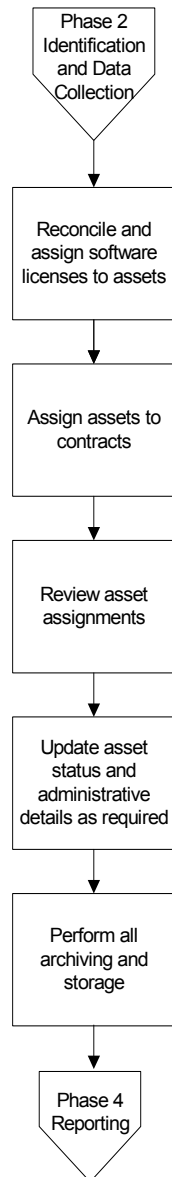
Phase 4: Reporting

This section details the Reporting phase.

1 Determine report requirements.

2 Produce reports.

Generate reports using available data. Use queries to filter information for generating reports. These include maintenance reports, internal reports, client reports, and ad-hoc reports.

Reporting Workflow

```
        ┌─────────────┐
        │   Phase 3   │
        │  Inventory  │
        │ Maintenance │
        └─────────────┘
               │
               ▼
        ┌─────────────┐
        │ Determine   │
        │ report      │
        │ requirements│
        └─────────────┘
               │
               ▼
        ┌─────────────┐
        │  Produce    │
        │  reports    │
        └─────────────┘
               │
               ▼
```

| Produce maintenance reports | Produce internal reports | Produce client reports | Produce ad-hoc reports |

```
               │
               ▼
        ┌─────────────┐
        │   Phase 5   │
        │ Verification│
        │  and Audit  │
        └─────────────┘
```
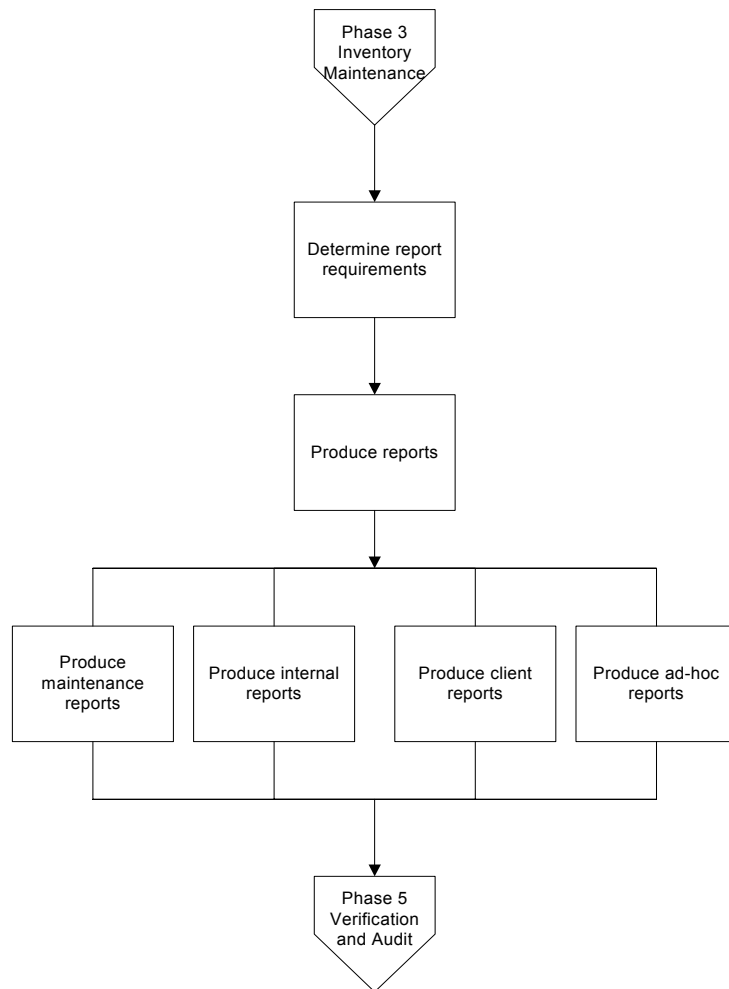
Phase 5: Verification and Audit

The following steps guide you through the Verification and Audit phase.

1 Check data standards

   - Identify Components
   - Update legacy assets
   - For configuration structures, describe the relationship and position of components.

2 Make amendments

   - Update data if there are changes. Each time a change or task is updated, all linked records are automatically updated with current details.

3 Run a Change Management comparison report.

   - Changes to asset data could result from the RFC process or an asset's properties changing since the last scanning. The relevant fields are mapped and each change or task record will generate a separate record against an asset. Each time a change or asset is updated, the relevant record is updated with the current details.
   - The generated report should show:
     - Asset Tag
     - Status Change Date
     - Change Number
     - Change Status
     - RFC number
     - Description of change
     - Values that have been affected by the change

4 Review the Change Management comparison report

   - Use the comparison reports to identify component differences that don't have correlating entries in the CM descriptions.
   - If descriptions match, accept the record as correct
   - Check the changes against RFCs. If there is no match, the change is classified as *unauthorized*.

Verification and Audit Workflow

```
                    ┌─────────────┐
                    │  Phase 4    │
                    │  Reporting  │
                    └─────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Check data  │◄──────────────────┐
                    │ standards   │                   │
                    └─────────────┘                   │
                           │                          │
                           ▼                          │
                        ╱──────╲                ┌──────────────┐
                       ╱Standards╲    no        │ Investigate &│
                       ╲ passed? ╱─────────────►│   resolve    │
                        ╲──────╱                │  exceptions  │
                           │                    └──────────────┘
                          yes
                           ▼
                    ┌──────────────┐
                    │Compare data  │◄──────────────────┐
                    │ via CM       │                   │
                    │comparison    │                   │
                    │  report      │                   │
                    └──────────────┘                   │
                           │                           │
                           ▼                           │
                        ╱──────╲                ┌──────────────┐
                       ╱ Accept  ╲    no         │ Investigate &│
                       ╲ the     ╱──────────────►│   resolve    │
                        ╲change?╱                │  exceptions  │
                        ╲──────╱                 └──────────────┘
                           │
                          yes
                           ▼
                    ╭──────────────╮
                    │     End      │
                    ╰──────────────╯
```
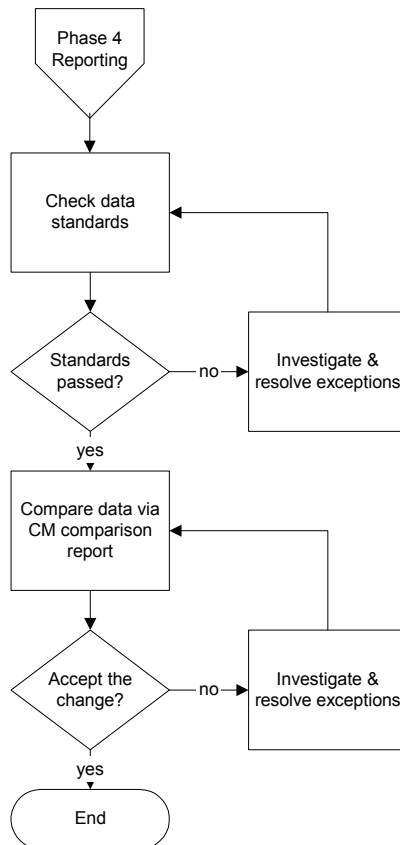
6 Service Level Management

CHAPTER

The objective of Service Level Management (SLM) is to maintain the optimum level of IT services through a good working relationship between the provider and the client. The optimum level of service is provided when the client's needs and requirements are met in terms of speed and correctness of IT services.

This chapter describes how to use Service Level Management to track performance of service agreements and contracts between customers and service providers.

Topics in this chapter include:

Introduction

Service Level Management (SLM) tracks performance of Service Level Agreements (SLAs) and contracts between customers and service providers.

An SLA might be either internal (between departments within the same organization) or external (between an organization and a vendor). Service level agreements define two major facets of service:

- Availability of a specific resource, within a specified time frame.
- Performance guarantees for service response times.

SLAs enable service providers to:

- Create a service level agreement, including description, availability, and response details.
- Configure the display of graphs, automatic alerts, and escalations.
- Calculate outage records.
- Map SLAs to appropriate departments.

SLAs are integrated with other ServiceCenter applications for tracking performance against established SLAs.

- For Service Management, SLA identifies the level of service to extend to a particular caller.
- Similarly for Incident Management, SLA determines the level of service to be provided to a particular customer. Open incident tickets display SLA guarantees and current response metrics.

For Inventory Management, SLA provides a complete outage history for each object (device), and automatically tracks its availability.

An SLA might be either internal (between departments within the same organization) or external (between an organization and a vendor). Service level agreements define two major facets of service:

- Availability of a specific resource, within a specified time frame.
- Performance guarantees for service response times.

SLAs enable service providers to:

- Create a service level agreement, including description, availability, and response details.
- Configure the display of graphs, automatic alerts, and escalations.

- Calculate outage records.
- Map SLAs to appropriate departments.

SLAs is integrated with other ServiceCenter applications for tracking performance against established SLAs.

- For Service Management, SLA identifies the level of service to extend to a particular caller.
- Similarly for Incident Management, SLA determines the level of service to be provided to a particular customer. Open incident tickets display SLA guarantees and current response metrics.
- For Inventory Management, SLA provides a complete outage history for each object (device), and automatically tracks its availability.

For further details about using and setting up Service Level Management, see the *Request Management Guide*.

Service entitlement

When a call or RFC is first logged, the user is asked to provide specific information for validation of entitlement to service. This information can include name, employee or asset number. The call is rejected if the user's entitlement to service can not be verified.

Note: Make sure there is a set process for maintaining user data to ensure that service is not wrongly rejected.

User authentication

When a password reset is requested, the user is asked for information to verify his/her identity. Typical identifying information can range from an employee number to personal information.

User authentication is part of the security policy of the service and is agreed upon prior to service commencement.

Critical users and equipment

Critical Users are client staff who perform vital tasks for some or part of the time. Downtime for these users has a greater business impact than downtime for standard users.

Critical Equipment items are devices that perform vital business functions. This would include the most shared items such as file/print and application servers, and enterprise printers, as well as high-end workstations such as a CAD station.

Site category definitions

Critical Site—Large site or campus location that justifies on-site support resources. A critical site routinely requires extended hours of support.

Major Site—Medium size location that justifies resources support by field-based technicians

Satellite Site—Small location supported by field-based or visiting technicians

Home Site—Home location of remote or field based user. This site is supported by field-based or visiting technicians.

Service hours

If service is requested of on-site support, requests are confined to the hours supported for that site. When requests are logged outside of normal support hours, service is performed at the beginning of on-site support hours.

Mobile and home users

When mobile or home users need support, they first contact the help desk. From there, the help desk and the user agree on the level of support required to resolve the issue.

A mobile user cannot be considered a critical user. This affects the severity level of the Incident.

7 System Set-up and Administration

CHAPTER

ServiceCenter system administration involves:

- Installing the software for clients, server, and database.
- Setting up operators and applications.
- Administering and maintaining the system.

Topics in this chapter include:

System Installation

The ServiceCenter server can be installed on a range of operating systems, including:

- Microsoft Windows
- Unix
- OS/390 (MVS)

Both Java and Windows clients are available. For further details of platforms and clients, see the range of installation guides listed in Chapter 5.

The out-of-box ServiceCenter database is PeregrineFour (P4). This can be mapped to a range of external RDBMSs, depending on the operating system, including:

- DB2 Universal, for Windows, Unix, and OS/390
- Oracle, for Windows and Unix
- Sybase, for Windows and Unix
- Informix, for Windows and Unix
- Microsoft SQL, for Windows

For further details of database set-up, mapping, and conversion, see the *Database Management and Administration Guide*.

System and Application Set-up

Once servers, clients, and the database are installed, the system administrator can set up:

- Time zone and date formats (see *Setting Time Zone and Date Formats* on page 111).
- User access to the system and to specific modules (see *User Access* on page 111).
- Print routines and printers (see *Print Routines and Printer Set-up* on page 112).
- An interface to Lightweight Directory Access Protocol (LDAP) directories (see *Lightweight Directory Access Protocol (LDAP)* on page 113.
- Data security - Mandanten (see *Data Security - Mandanten* on page 113).

- File size limits (see *Defining File Size Limits* on page 114).
- Computer-telephone integration (see *Telephony* on page 113).
- Clocks, for tracking the time of specific types of activities (see *Setting up Clocks* on page 114).
- Data in support files (see *User Access* on page 111).

Details of application-specific set-up can be found in the *Application Administration Guide* and the *Request Management Guide.*

Setting Time Zone and Date Formats

Out-of-box ServiceCenter includes information for time zones around the world in the tzfile. These can be modified and new ones can be added as required. The tzfile enables automatic clock adjustment during time zone switchovers, for example, between Standard Time and Daylight Savings Time.

The system administrator can set a default time zone and date format for the overall system, as well as set specific ones for individual operators.

- Select date format for local requirements. This is set as a default in the company record (see *Company File* on page 116).
- Specify requirements for individual operators, via the operator record (see *User Access* on page 111). This enables remote ServiceCenter users, based in other time zones and countries, to view date/time information converted to their local time and date formats.

For further details on setting time zones and date formats, see the *System Administrator's Guide.*

User Access

The Central Administration Utilities (CAUs) enable system administrators to grant users system access and functionality within applications, via the operator file and the company record. The CAUs also provide for the central definition of user profiles, assignment groups, and message groups.

The company record contains information used by the applications accessing the server. It defines several server-wide aspects, including:

- Logical file size limits.
- Login and password limits and standards.

- The setup for the `syslog` audit trail.
- The default time zone, date, and month formats.
- Length of time for queries.

The `operator` file contains operator records with the login name, password, and capability words for each user. Capability words define the functionality that the user is allowed. The operator record also includes the profiles that define the functionality within an application to which a user has access.

Out-of-box ServiceCenter includes user roles with associated profiles to expedite setting up appropriate user access and privileges within each application.

For further information about how to set up user access and data security, see the *System Administrator's Guide* and the *Application Administration Guide*.

Print Routines and Printer Set-up

ServiceCenter provides enhanced print routines (*us.print* routines) for use with most of the primary application modules for printing from the database, as well as both client and server printing.

The enhanced routines provide fast and robust printing, automatically expanding array fields to print each line of an array. Records spanning multiple pages are printed with page numbers.

ServiceCenter can be set up to:
- Print a form (the screen as currently displayed), along with the data in the form.
- Print a record from an application, including all information contained in the record. Printers used by clients and servers are defined in a configuration file.

For an explanation of print routines and how to set up printers, see the *System Administrator's Guide*.

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) directories provide a centralized source for information about the people within an organization, such as email addresses, telephone and fax numbers, user IDs, and passwords. They can eliminate the need to maintain user data in more than one location.

ServiceCenter has been configured to interface with LDAP directories to simplify the creation of operator records for large groups of users. It is available on all platforms except OS/390.

For details of the LDAP server interface, see the *System Administrator's Guide*.

Data Security - Mandanten

ServiceCenter's Mandanten enables protection of records for multiple clients by separating a shared database. Those using a specific client see only the data they are allowed to share. Protection can be further applied within client groups, enabling system administrators to conceal department records selectively within an organization.

Mandanten is set up by defining lists of field values for disparate users that access the same database. These values are assigned to security groups named in the operator record and then associated with a mandanten field in the ServiceCenter file to be protected. Several security groups can be named in the operator record for a given user.

For details of how to set up mandanten protection on fields, see the *System Administrator's Guide*.

Telephony

ServiceCenter Telephony (SCT) provides options for computer-telephone integration so that workstations can be set up to answer incoming telephone calls. Using Microsoft's Telephone Application Programming Interface (TAPI), ServiceCenter Telephony enables a user, by a click of the mouse, to:

- Answer a call.
- Place a caller on hold.
- Return to the call or hang up.

For details of setting up telephony, see the *System Administrator's Guide*.

Defining File Size Limits

System administrators can limit the size of attachments, records, and arrays by defining file size limits in the operator record, the company record, and in Forms Designer (a tailoring tool, as described in Chapter 4).

Logical size limits can be set in the initialization file (sc.ini) to prevent record sizes from becoming too large and from large arrays being built.

For details of how to define file size limits, see the *System Administrator's Guide* and *System Tailoring*.

Setting up Clocks

ServiceCenter clocks, as defined in the clock file, enable tracking of time for specified activities, for example:

- The time that an incident ticket remains in a given state: **Open**, **Pending**, and the **Total** time.
- The time an operator spends editing a ticket.
- The time it takes for a ticket to be worked by a given assignment group or multiple groups.

For details of how to define file size limits, see the *System Administrator's Guide* and *System Tailoring*.

ServiceCenter Support Files

System administrators can directly access the following support files (and their options menus) used in the administration of ServiceCenter.

- Contacts (contacts file)
- Location (location file)
- Model (model file)
- Vendor (vendor file)
- Company Information (company file)
- Department (department file)
- Currency (currency file)
- Currency Conversion (curconvert file)

These files supply ServiceCenter's principal applications with data that the users may query or use to easily populate fields using the *Fill* function.

The system administrator can create, update, and delete records from the ServiceCenter support files. For details about these tasks, see the *System Administrator's Guide* and the *Application Administration Guide.*

Contacts File

The contacts file stores information about individuals who call the help desk and other individuals who may be contacts for incident tickets, change requests, request quotes, and inventory records. This information is used throughout ServiceCenter to provide complete contact information for items or activities, such as opening incident tickets, change requests, and inventory records. Typically, contacts are also associated with certain devices, which simplifies the task of opening a call report, an incident ticket, or a change request.

Location File

ServiceCenter contains a location file with records listing information such as the physical address of components, location code, contact, and hours. This data is used to fill in the location information in records in other ServiceCenter applications, such as an incident ticket in Incident Management.

Model File

ServiceCenter contains a model file to track different models of components in a network. For example, the model file is linked to device records in Inventory Management. The model file is also linked to ServiceCenter's Request Management (see the *ServiceCenter Request Management Guide* for details). The model file is the core of the Request Management catalog. When model information is stored in Request Management, users can learn:

- Rules for processing a component as a line item, part of a quote, or order.
- Rules for selecting the components of a parent part.
- Dependencies.
- Approvals required when a component is part of a quote or order.
- Quantities of a component that are in use, on hand, on order, and so on.

Vendor File

The ServiceCenter vendor file stores records of vendors, manufacturers, and contractors — the data necessary for contacting and working with vendors.

The vendor file information is linked to several Request Management files (for example, quote, order, and line item) where the information is placed in the **Vendor** field. This file is also linked to the **Service Provider** field in an incident ticket, to the **Manufacturer** field in the model file, the **Vendor** field in the device file, and to the **Vendor** field in the modelvendor file.

Company File

Company information contained in the company file is used throughout ServiceCenter to complete forms and validate fields, such as fields in Contract Management. Unlike the *company record*, which stores particulars about ServiceCenter sites, the company file contains basic location and contact information about other companies with which the organization has contractual relations.

Department File

The department file records basic data about the various departments within your organization, including the internal service level agreement. It can also include a graphic for the departmental organization. Department records can be accessed from other ServiceCenter files, using the *Fill* function.

Currency File

The currency file defines a name, code, display format, and description for each currency used in the system. Currency definitions are used in conjunction with conversion rates (see the curconvert file description). The currencies defined in the currency file are used to name the currency used for calculating values in the model file. The cost per unit is figured using the currency listed in the **Currency** field.

Currency Conversion File

The curconvert file provides currency exchange rate information through the currency conversion utility that automatically converts 166 national currencies, depending upon exchange rates at the time the contract is granted. Daily exchange rates can be entered into the system, ensuring accurate rate conversions. Contract Management manages all currencies in compliance with European Union currency regulations.

Day-to-Day Administration

As part of day-to-day responsibilities, system administrators are called upon to:

- Set server control parameters (*Maintaining Server Operation*).
- Search for specific records (see *Searching for Records* on page 117).
- Monitor the status of the system (see *Monitoring System Status and Events* on page 118).
- Create Hot News entries to highlight current high-profile tickets (see *Creating Hot News Entries* on page 119).
- Load, unload, import, and export (see *Transferring Data To and From ServiceCenter* on page 119).
- Purge and archive data (see *Purging and Archiving Data* on page 120).
- Balance the load among several servers (see *Load Balancing* on page 120).

Maintaining Server Operation

System administrators can set control parameters on the server to control how connected clients work for printing, viewing, and saving. These are maintained centrally in the sc.ini file for the server. Setting these centrally disables the ability of an individual user to control these options via the client.

For details of how to change server control parameters, as well as starting and stopping servers, see the *System Administrator's Guide.*

Searching for Records

Query-by-example (QBE) search is initiated by entering values or a range of values in the fields on a blank form, then clicking Search or pressing Enter.

The system searches key and non-key fields, then displays a QBE list of all records that satisfy the search query. The key fields are listed across the screen. If the QBE list is too long to fit on one screen, the system allows the use of scroll keys to page through the list. If the search criteria uniquely defines a record, the system immediately displays that record.

Advanced Search

Advanced search provides:

- Additional fields for qualifying the search.
- The time frame for when a record was opened or updated.
- Names of the operators who opened or updated the report.

These fields are independent of each other and can remain blank. For further details of how to search for records, see the *User's Guide*.

Monitoring System Status and Events

ServiceCenter provides a system status window to facilitate:

- Checking the status of a background process.
- Monitoring which users are currently logged on.
- Halting a user's session or task.
- Checking system locks.
- Sending out broadcast messages.
- Starting the scheduler for background processes.
- Viewing statistics of ServiceCenter processes.

For further details of the System Status window, see the *System Administrator's Guide*.

Additionally, ServiceCenter enables system administrators to be proactive in monitoring events to ensure peak system performance, without having to search through messages in the log file manually. This is done by:

- Setting up the Alert Periodic scheduler to check on virtual memory consumption and the size of various queues at a specified frequency. This is done via the Database Manager in the Toolkit (see *Database Manager* on page 129).
- Setting up the alert categories and descriptions for reporting alerts in the log.
- Setting up the parameters in the sc.ini file to specify the conditions and timings for raising alerts, including:
  - Average CPU usage for a user.
  - Number of records in the ServiceCenter Distributed (SCD) data queue.
  - Length of time for a system lock.

- Number of records in an IR queue before causing an alert.
- Path for location of the system log file (typically the RUN directory) where alerts should be recorded.
- The amount of time that a query can execute before an alert is written.
- Number of records in an SQL Shadow queue.
- Maximum amount of memory that can be used.
- System wait time, the amount of time that a client is waiting for resources.
- Parameters to be filtered out and not reported.

- Setting up the message log switch, specifying the frequency with which a new log file is created so that files are kept to a workable size and can be archived.

For further information about how system events are monitored, see the *System Administrator's Guide*.

Creating Hot News Entries

Hot News entries are designed to present 'late-breaking' information such as server outages and other infrastructure failures to help desk operators. These are displayed in Service Management and Incident Management forms.

For details of how to set up a Hot News entry, see the *System Administrator's Guide*. For information about of how to use Hot News entries, see the *User's Guide*.

Transferring Data To and From ServiceCenter

Several functions are available for moving data into and out of ServiceCenter.

- Unload - a function within Database Manager for extracting one or more records, a QBE, or a dbdict from ServiceCenter for eventual re-loading into the same or another ServiceCenter system. By convention, the file extension for unloads is .UNL. An utility facilitates unloading by enabling creation of a query list for classes of records. The query list can be retained for subsequent use.
- Load - a function for transferring an unload file back into ServiceCenter.

- Import - a utility for importing specified fields from an external flat, sequential, fixed-length file (for example, a Microsoft Excel file) into a ServiceCenter file. A wizard facilitates importing of fixed-width or comma-delimited text files. Import can be run in the foreground or scheduled as a background process.

- Export - a utility for extracting fields from ServiceCenter to a file for use by an external system. Text files and Microsoft Excel files can also be created via DDE.

For additional details about loading, unloading, importing and exporting data, see the *System Administrator's Guide* for details. For DDE capabilities, see *System Tailoring*.

Purging and Archiving Data

The purge and archive functions enable system administrators to control the database size by extracting older records for external storage. Periodic archiving (extraction) of records can be scheduled at off-peak hours as a background process, followed by purging of those records from the active database. Data maps, tracking the hierarchy of relationship between primary and secondary records, are produced and used to ensure integrated removal of related records.

For an explanation of how to purge and archive data, see the *System Administrator's Guide*.

Load Balancing

ServiceCenter's Load Manager enables system administrators to balance the requirements for CPU and memory usage across multiple servers running on multiple platforms. It manages the resources used among the servers and monitors users, licensing, and resource locking.

For further information about Load Manager, see the *System Administrator's Guide* for details. Since Load Manager requires a relational database management system, see also *Database Management and Administration* for details.

8 Tailoring ServiceCenter

CHAPTER

Once ServiceCenter is installed and set up, there might still be further changes desired for site-specific requirements, including special field validation, new or modified forms design, expanded or varied workflow, and automatic notifications. ServiceCenter includes a range of tailoring tools for on-site developers to use.

Because these tools enable extensive changes to ServiceCenter, careful analysis is recommended before implementation, balancing the gains of tailoring against ease of upgrading to future out-of-box releases. ServiceCenter utilities, like the Document Engine, Revision Control, and Revision Tracking, facilitate stable and well-documented tailoring and upgrades.

Topics in this chapter include:

- *What is Tailoring?* on page 122
- *Tailoring Tools* on page 124

For details about most of ServiceCenter's tailoring tools and utilities, see ServiceCenter *System Tailoring*. References to other guides are included in the specific sections.

What is Tailoring?

Tailoring is any change to out-of-box functionality beyond the setting of parameters, without changing actual code. For example,

- Changing the default values for items that appear (or not) on forms (window layouts) and are used for field validation, See *Setting Default Values* on page 124.

- Creating and using macros, scripts, and stored queries (see *Macros, Scripts, and Stored Queries* on page 127).

- Adding or changing the look and operation of forms, including changes to record definitions. See *Adding or Modifying Forms and Records* on page 128.

- Adding or changing automatic messaging. See *Forms Designer* on page 128.

Rapid Application Development (RAD) Code

ServiceCenter is written in Rapid Application Development (RAD) code, a proprietary language developed and owned by Peregrine Systems, available only by special license.

Most tailoring can be done using high-level ServiceCenter tools, without directly changing the RAD code.

Controlling Changes with the Document Engine

The Document Engine is a facility within ServiceCenter that enables manipulation of common RAD code sets and algorithms, without making direct changes to the code. This ensures safe and predictable changes. The Document Engine is used with several tailoring tools, including the Database Manager, Format Control Editor, Link Editor, and Revision Control.

The Documentation Engine currently supports tailoring for Service Management, Incident Management, Change Management, and Request Management. System changes can be effected across one or more of these modules.

Safeguarding the System with Revision Control

During the tailoring process, Revision Control enables developers to restore the original configuration of a file, format, or even the whole system, if required. Since Revision Control is part of the Document Engine, it is available for use with any of the Document Engine utilities. It is also available for use with the Forms Designer and the RAD Editor.

Tracking Changes with the Development Audit Utility

The Development Audit Utility (also known as Revision Tracking) records changes in system files important to tailoring, for example, application files, code files, datadict files, displayoption files.

Revision Tracking stores a record for each record added, updated, or deleted in any of these files. Developers can monitor the volume of changes, creating an unload of the changes at appropriate frequencies.

Creating Unload Files for System Upgrades

Developers can use the Utility to expedite creation of standard ServiceCenter unload files (by convention, with an extension of .UNL) for moving the changes from a development system to production. Features include the ability to unload:

- Features and files, such as forms, link records, and Format Control records, intact to the new system.
- Entire classes of records, as a single file.
- The record itself, thereby keeping the query list intact for further upgrades or data swapping.

Tailoring Tools

Following is a brief overview of tools available for tailoring ServiceCenter. Although these have been grouped into general categories, some tools can be used for several different types of changes. Conversely, there may be multiple ways to achieve a given system change. For details of how to use the tools, see *System Tailoring*.

Setting Default Values

Default values drive the automatic appearance of items on forms, values in required fields, and the visibility of items to specified users. These are tailored using:

- Format Control (see *Format Control Utility* on page 124), including Sequential Numbers and Data Validation.
- Data Policy (see *Data Policy Utility* on page 126).
- Display records (see *Display Application* on page 126).
- Global lists (see *Global Lists Utility* on page 126).
- Menus (see *Menu Manager* on page 127).
- Links (see *Link Utility* on page 127).

Format Control Utility

Format Control enables developers to apply special processes to ServiceCenter files through individual forms, including:

- Field validation.
- User privileges.
- Display of alternate QBE forms.
- Calculations and validations based on fields in other parts of the database.
- Calls of RAD routines.
- Definition of additional options and menu items.
- Automatically updating or insertion of data in other parts of the database.

Format Control records can be attached to any form or file within
ServiceCenter and do not require special programming skills to implement.
Routines defined in Format Control can be user-interactive or transparent.
The activated when a record is displayed or when a user adds, updates, or
deletes a record from the database.

Format Control is easily applied and changed and is intended as a convenient
utility, but should not be overused. Excessive reliance on Format Control to
modify the system can result in reduced system performance. An alternative
is to use Data Policy instead for certain types of changes (see *Data Policy
Utility* on page 126).

Sequential Numbers

Sequential numbers is a subroutine process of Format Control that
automatically adds identifying numbers to database records, as they are
created. For example, sequential numbering can be used for inventory
control, incident tickets, or employee records.

Data Validation

Data validation is used to validate data within specified fields of
ServiceCenter applications to improve efficiency and ensure quality of
information. Data validation is specified in validity records that are called
from Format Control.

For example, fields in Incident Management might need to be validated to
improve the efficiency of opening tickets. Typical Incident Management
validations are:

- Ensuring that a field matches certain criteria (for example, **open.date**
  <=current date and time).
- Checking that the content of a field matches an element of a list of
  acceptable values (for example, **contact.name** must be a valid contact
  name).

Data Policy Utility

Data Policy is a standard ServiceCenter utility used for defining and enforcing overall data rules for individual files. It operates at the table level and can achieve many of the same results as Format Control without the complexity and without taxing system resources.

Data Policy provides a simple interface through which developers can apply default values, mandatory fields or lookup validations to a specific table. These policies, once set, will be enforced across the entire system, regardless of what form is being used to display the data.

Display Application

The Display application enables developers to customize a range of features without altering RAD code. Datafiles within Display contain the individual records (known as displayscreen records) in which options, events, and window controls are defined.

Screens

A displayscreen record defines the attributes of a screen and provides the user with access to the individual records for options and events.

Note: A screen is not the same as a *form*. In Display Screens, screens are individual records identified by a unique Screen ID.

Options

Display options can appear in the Options menu or as System Tray buttons in GUI mode (Windows and Java client) and as function keys in Text mode. Various display options can be set in the displayoption file.

Events

Display events defines the *events* a screen will handle. Definitions, such as conditions and expressions, can be set in the displayevent file.

Global Lists Utility

The Global List utility enables creation of lists that are available to any ServiceCenter application module. For example, a global list might be used as the combo box to a form that displays a list of operators based on a table in the database.

Menu Manager

The Menu Manager is used to define all menus in the system. Each menu consists of one record residing in the Menu file. Access to menus and menu items depends on the user's profile, as defined in the operator record.

Link Utility

The Link utility enables creation of relationships between files in ServiceCenter modules in which information should match. For example, a file in ServiceCenter's Inventory Management can be linked to another file in Incident Management, helping to combine data and link definitions, setting the conditions to create the relationships for linked information.

Macros, Scripts, and Stored Queries

Developers can use macros, scripts, and stored queries to automate processes and tailor the accessibility of information for particular users.

Macros

Macros are distinct actions, driven by predefined conditions, that execute when a record is saved in the database. They are created using the ServiceCenter Macro utility. Macro actions are associated with files and reflect certain states in the records of those files.

Scripts

Scripting is a utility that enables interruption of the normal screen flow to display a series of forms, or execute some decision-tree processing, without modifying the original RAD code.

Scripting is particularly applicable for a process that requires a user to supply a pre-determined set of information since the screen flow within a script can be based on user-entered data.

Depending on how a user replies to a question (such as, "Are you reporting a printer problem or a terminal problem?"), scripting can determine the screen to display next. While the script is executing, the user-entered data is accumulated in a file variable, which is returned to the calling application when the script is complete.

Dynamic Data Exchange (DDE) Scripts

ServiceCenter supports use of Microsoft Windows Dynamic Data Exchange (DDE) in two ways:

- ServiceCenter acting as a DDE server, enabling an external Microsoft application to 'get and set data' (DDE Request and DDE Poke, respectively). The initiating application is the external one, for example, Excel.

- Using the DDE Script panel, ServiceCenter can initiate DDE calls to external applications.

Stored Queries

The Stored Query Maintenance utility enables designated users to define and store queries that define the display lists of specific records or populate dynamic display objects such as charts and marquees.

For example, stored queries can be created to search for incident tickets that have reached a certain status, to populate a chart that displays open tickets by category, or to display a list of change requests assigned to a particular approval group.

Adding or Modifying Forms and Records

A form is the GUI screen layout used to add, change, and view ServiceCenter records in a file. (In ServiceCenter, 'form' is synonymous with 'format'.) Developers can add or remove buttons, marquees, and fields on any form, as well as determine which form appears, based on a user's role.

Forms Designer

Forms Designer is used to design, create, and update ServiceCenter forms, including:

- a Drawing Canvas, for constructing forms.
- a Tools Palette, for creating design objects.
- a Properties Window, for setting attributes for each object.

In addition, Forms Designer has a Form Wizard, used to create forms automatically, based on a particular database dictionary (for further details, see the *Database Dictionaries (dbdicts)* section below.

Database Dictionaries (*dbdicts*)

The database dictionaries, referred to collectively as the dbdicts, define the ServiceCenter database logical files. A file is created by generating its dbdict record.

The data can either be tailored manually using the dbdict tool, or using **Create file** in Forms Designer, based on a format containing all currently known fields (the dbdict is automatically generated using this method). A file can be created or modified, adding fields to existing file to store additional information on the specified records, for example, incident tickets or inventory records.

Database Manager

The Database Manager is used to create and access data records using ServiceCenter forms. All ServiceCenter data and system-defined information are stored as records in files. Forms that have been associated to a file are available to users for viewing and manipulating data.

Using the Database Manager, any appropriate file may be accessed with a single function key. When a file is uniquely defined, the system immediately displays the format for that file. If the file name is not uniquely defined, the system displays a QBE list of files, satisfying the search argument for you to select the file you want to view.

The Database Manager takes a screen format and its associated database dictionary (dbdict file) and allows access and management of the database at three levels:

- At the single-record level, the ability to add, update, delete, retrieve, load, and unload individual records.
- At the multiple-record level, the ability to perform all the single-record functions on a subset of the records in a database.
- At the file level, the ability to rebuild the keys to a database file or empty a database file.

For further details of how to use Database Manager, see the *Database Management and Administration Guide*.

Audit Specifications

Auditing enables a user to check specified fields within a file in the ServiceCenter database for any modifications. It notes when records in that file are updated.

The *Audit Specifications* file provides instructions on how and when to perform an audit, and it defines files and fields to be monitored by the Audit utility. There is one specification record for each dbdict file.

Generating Automatic Notifications and Publishing Messages

ServiceCenter has utilities to facilitate generating notifications triggered by system activity and broadcasting messages to users.

Notifications

The Notification Engine is primarily responsible for sending messages that are generated by ServiceCenter events, such as opening or closing an incident ticket. Developers can edit these messages, add new messages, change the conditions under which the messages will be sent, as well as select who will receive the messages.

The Notification Engine, as a centralized message utility, has several advantages:

- Consistency in messages across ServiceCenter modules.
- Easy update and customization.
- The ability to tailor notifications with RAD expressions, without jeopardizing the integrity of the RAD code or requiring a RAD license.

Publishing Utilities

Publishing Utilities use agents, special background processes that perform certain tasks for the user, to publish simple, static messages and marquees to any ServiceCenter form.

For example, a static message could be attached to a menu for notifying a designated group of users of the average time for resolution of an open ticket.

9 Further Information and Support

CHAPTER

A range of documentation in various media and several training courses are available from Peregrine Systems. Customer Support is also available.

Topics in this chapter include:

- *ServiceCenter Documentation* on page 132
- *Peregrine Education Services* on page 134
- *Contacting Customer Support* on page 135

ServiceCenter Documentation

A full range of documentation is available for ServiceCenter for installation, system and application set-up and administration, and tailoring.

General

- *Release Notes*
- *Introduction & Best Practices**

Installation and Upgrade

- *Client/Server Installation Guide for Windows*
- *Java Client Installation Guide*
- *Client/Server Installation Guide for Unix*
- *Distributed Services Quick Start Guide*
- *Client/Server Installation Guide for OS/390 (MVS)*
- *SC3270 Client Installation Guide*
- *Upgrade Implementation Utility*

System Set-up and Administration

- *System Administrator's Guide**
- *Database Management and Administration Guide**
- *Application Administration Guide**
- *Event Services**
- *Technical Reference**

Day-to-day Service Provision

- *User's Guide**
- *ReportCenter Guide**
- *Request Management Guide**
- *Work Management Guide**

System Tailoring

- *System Tailoring**
- *Rapid Application Development (RAD) Guide* - available only to license-holders

*Available as online guides (HTML format).

Media Availability

All documentation is available in softcopy, printable (PDF) format (see *Printable Guides* on page 133).

ServiceCenter software is shipped with a printed and bound set of installation guides, plus the Release Notes. Online guides (HTML format) are available for most standard, non-installation documentation (see *Online Guides* on page 134).

Printable Guides

A complete listing of ServiceCenter documentation is available on at:

   http://support.peregrine.com

After logging in with your login and password,

1 Select **Go** for **CenterPoint**.

2 Select **ServiceCenter** from **My Products** at the top of the page.

3 Then, from **Contents** on the left, select either **ServiceCenter Product Documentation** or **ServiceCenter Product Release Notes**, as required. Follow the path for the ServiceCenter version and category of documentation that you need.

For printable copies of the manuals, you can download PDF files of the documentation using the Adobe Acrobat Reader (available from *www.adobe.com*).

Additionally, you can purchase printed and bound copies of the documentation through Customer Support (see *Contacting Customer Support* on page 135).

Online Guides

The default installation for ServiceCenter on Windows and Unix platforms includes downloading of online guides in HTML format. (For a list of the online guides, see *ServiceCenter Documentation* on page 132.)

Online documentation is also an option in the custom installation.

To access the online guides in a Windows installation:

1   Select Start>Programs>ServiceCenter>Documentation.

2   Click on the title of the online guide that you wish to view.

3   Instructions for navigating within the online guides are included at the start of each document. A table of contents shows on the left. Click a topic to display it. Other search and index options are also available.

Help Text

ServiceCenter's Help utility allows organizations to include site-specific field-level help. Additionally, out-of-box help is provided in ServiceCenter 5 for fields in Service Management and Incident Management workflows.

Peregrine Education Services

Education Services offers a range of courses to ensure that technical administrators and implementation staff can perform at their highest level and maximize their organization's investment in Peregrine's solutions.

The catalog of courses supports an organization's development through all four levels of service management. Education options use a proven, blended-learning model that includes:

- Computer lab courses at Peregrine's world-class training facilities.
- Self-paced Web-based training.
- Live and recorded Internet sessions.

All training is facilitated by expert instructors.

ServiceCenter technical courses are designed to meet the needs of various roles, including system administrator, developer, and manager.

Courses currently available include:

- Introduction
- ServiceCenter Tailoring
- System Administration
- Change Management
- Request Management
- Service Level Agreements
- ServiceCenter DVD and the Display Application
- ServiceCenter Automate Lab
- Upgrade Lab
- Rapid Application Development (RAD)

Customer site training, customized classes, and end-user training are also available. Detailed information about all courses, suggested course sequences, and registration information is available at:

http://www.peregrine.com/education/

Contacting Customer Support

Current details of local support offices are available through the following main contacts or at *http://support.peregrine.com*.

After logging in with your login and password:

- Select **Go** for **CenterPoint**.
- Select **Whom Do I Call?** from **Contents** on the left side of the page to display the **Peregrine Worldwide Contact Information**.

Corporate Headquarters

All countries other than Europe, the Middle East, and Africa (EMEA) can contact Customer Support at Peregrine corporate headquarters as follows:

Address:	Peregrine Systems, Inc. Attn: Customer Support 3611 Valley Centre Drive San Diego, CA 92130 USA
Telephone:	(1) (800) 960-9998 (USA and Canada only, toll free) +(1) (858) 794-7428
Fax:	+(1) (858) 480-3928
E-mail:	support@peregrine.com

Europe, Middle East, and Africa (EMEA)

All countries in Europe, the Middle East, and Africa (EMEA) can contact Customer Support at:

Telephone:	+44 (0) 800-834-7700 +44 (0) 208-334-5844
E-mail:	uksupport@peregrine.com

Glossary

Terms Used in the ServiceCenter Interface and Documentation

Term	Definition
Access Control List (ACL)	A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Microsoft Windows NT/2000 and Unix-based systems are among some of the computer operating systems that use access control lists. Each object has a security attribute that identifies the access control list, which, in turn, has an entry for each system user with access privileges. The most common privileges include the ability to read a file(s) in a directory, write to the file(s), and execute the file(s).
ACL	See Access Control List (ACL).
Active Notes	A ServiceCenter dialog box that displays messages in a pop-up window.
activity type	A user definable field used in Incident Management (IM) to indicate the reason for an update to an incident record. Activity types are maintained in the activity type file and can be used to trigger other events, such as an update to the status of an incident ticket. The use of Activity records and Activity type is an optional setting within the Incident Management Environment record to keep activity records of an incident record. This can be used in preference to paging (page list) in Incident Management.
adapter	See interfaces and adapters.
add	Create (insert) a new record in a ServiceCenter file.
administrative privileges	The rights assigned to the ServiceCenter user who maintains the system, granted via the sysadmin capability word.

Term	Definition
administrator	See system administrator.
Advanced Interactive Executive (AIX)	IBM's version of the Unix operating system.
affected hardware	Equipment, such as a PC, impacted by a change, incident, or other activity.
AG	See Application Generator (AG).
AIX	See Advanced Interactive Executive (AIX).
alert status	The current position of the ticket in the alert sequence.
alerts	Alerts support several functions within ServiceCenter. Alerts trigger a series of checkpoints taken against a change, task, quote, order, or line item to ensure that required work activities occur within specified time frames.
API	Application Programming Interface
Application Generator (AG)	The former name for Rapid Application Development (RAD).
applications application suite	ServiceCenter modules.
approval	An approval is the verification that the change or request process can start. Approvals allow the phases and the tasks in the phases to proceed. Without the approval in Change Management (CM), the life cycle of the change is put on hold. If certain tasks are not completed in the specified time frames, alerts are issued. Approvals can be approved or disapproved. In Request Management, the approval process automates and formalizes the evaluation of quotes and orders by the appropriate management entities. The approval process channels the risk, cost, and responsibility associated with the request to the proper levels. Approvals can either be approved, retracted, or denied.
approval group	The personnel responsible for accepting or disapproving the completion of a change, task, or phase. Approval groups are placed in sequences in the order that their approval is required. If groups have the same sequence number, their approvals can be made independent of each other.
approval sequence	The order in which approval requirements are made active. In Change Management (CM), the process first makes the lowest sequence numbers available for approval activity. Once these are approved, the next highest number is made available.

Term	Definition
approver	An approval group member who is authorized to approve or disapprove requests on behalf of the group.
asset	Component of a business process. Assets can include people, places, computer systems, networks, paper records, fax machines, etc. In the context of Incident Management (IM), assets are tracked in the device file, such as a device, software component, or piece of equipment.
assignment group	A user or set of users responsible for implementing a solution for an incident ticket. This group receives notification when an Incident ticket is opened or escalated.
associate	The ability to link different ServiceCenter record types. For example, calls can be linked to incidents reported in Root Cause Analysis on a one-to-one, one-to-many, or many-to-one pattern. Likewise, incidents can be linked to other incidents.
attachment	In ServiceCenter 4 and later, a file attachment associated with a ServiceCenter record and launched by double-clicking or using the right mouse button.
attribute file	A supporting file within Inventory Management (ICM) that holds data specific to a particular device type. If an attribute file exists for a device type, then each device record for that device type will have a corresponding attribute record in the device type's attribute file. For example, a switch attribute record might identify the maximum number of ports a switch can support and a modem attribute record would identify baud rate.
attributes	In the context of Inventory Management (ICM): each configuration item (CI) possesses a number of characteristics and features, which we call attributes. To set up the Inventory Management database, it is necessary to decide which attributes will be included.
authorization code	A series of unique numbers and letters supplied by Peregrine Systems, Inc. That enables user licenses and ServiceCenter functions within the appropriate modules. The authorization code is entered during the installation procedure and resides in the initialization file.
automatic refresh rate	The rate, in seconds, at which displayed queries are refreshed on the client screen. These are set up by the system administrator.
autosaving	ServiceCenter record updates that occur automatically when a user clicks the Back, Next, or Previous buttons or presses their corresponding keys.
availability	The percentage of time when a hardware, software, or other component is working as expected during its promised hours of operation.
Back button	The button that returns you to the previous Form.

Term	Definition
background agent	The process that runs in the background on the application server and performs assigned tasks.
background scheduler	See background agent.
binaries	ServiceCenter run-time environment system programs that run from a command prompt. This term is typically used in Unix environments.
BLOB	In the context of a Relational Database Management System (RDBMS), Binary Large Object. See CLOB and LOB.
browse	View without add or update capability.
btree	A hierarchical, forked file index organization.
build	In the context of Change Management (CM): the final stage in producing a usable configuration. The process involves taking one or more input configuration item (CI)s and processing them (building them) to create one or more output CIs, such as a software compile and load.
button	Graphical object that users click to initiate a ServiceCenter action, located in the system tray of a Form window or on the Form itself.
CA	Concept Approval
CAB	See Change Advisory Board (CAB).
CAB/EC	See Change Advisory Board/Emergency Committee (CAB/EC).
Calendar	The ServiceCenter Calendar is a collection of files supporting the definitions of working hours for different work groups. The work hour definitions and calendar files are as follows: Daily hours (caldaily) file Contains a definition for each work or assignment group for each day of the year and is used to calculate date intervals and alert dates. Duty hours (caldutyhours) file Defines the normal daily working hours for a particular work or assignment group. Holidays (calholiday) file Defines the starting and ending dates for valid company holidays. Note: Be aware of the time zone differences when executing events within ServiceCenter. Calendaring is based on a single time zone and will not compensate for time zone differences.
call	The means of establishing a line of communication with the Service Desk. A call record or incident ticket generated from a call to the Help desk. The ticket may be resolved by the call taker or the help desk team. It may also be associated with an incident record or known error record in Root Cause Analysis (RCA) or change record in Change Management (CM).
call record	The documentation of an issue in the ServiceCenter database.

Term	Definition
call report	A record opened in the Service Management (SM) module of ServiceCenter when a user calls the Help desk for assistance. ServiceCenter uses Service Management so that all calls get recorded, even if further action is not needed.
Capability word	A value in the Execute Capabilities section of an operator record that grants access to specific applications and utilities in ServiceCenter.
category	The classification within Change Management (CM) that classifies configuration item (CI)s, change documents, calls, incidents, quotes, and requests. ServiceCenter includes a series of default categories. Each Change record must have a category. system administrators can create new categories. Each category has at least one phase. See phase.
CAU	See Central Administration Utilities (CAU).
cause code	An optional code that links an incident ticket to a Probable Cause record. Cause codes allow incident tickets to be more easily categorized and assigned. By using a standard series of cause codes, users can simplify reporting and track incidents that have a common cause. The Cause Code field links a ticket to a related probable cause record. See also Probable Cause.
Central Administration Utilities (CAU)	A ServiceCenter tool for centrally managing ServiceCenter users, their access and security rights, and profile and assignment groups.
change	Another name for a change request or change record. The addition, modification, or removal of approved and supported items, such as hardware, network, and software.
Change Advisory Board (CAB)	In the context of Change Management (CM): a group of people who can give expert advice to Change Management on the implementation of changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units.
Change Advisory Board/Emergency Committee (CAB/EC)	In the context of Change Management (CM): when major problems arise, there may not be time to convene the full Change Advisory Board (CAB). It might then be necessary to identify a smaller organization with authority to make emergency decisions. Such a body is known as the Change Advisory Board/Emergency Committee (CAB/EC).
change authority	In the context of Change Management (CM): a group that is given the authority to approve changes.
change category	The basic building block of a change. The category defines the type of change that is requested.

Term	Definition
change initiator	In the context of Change Management (CM): the Change Initiator is the person who starts the process of a Request for Change.
Change Management (CM)	The ServiceCenter application module for administrative management of change records through the life cycle. Change Management is the ServiceCenter module in which root causes are resolved. The process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
change number	A unique tracking number assigned by Change Management (CM) when a change is submitted.
change owner	In the context of Change Management (CM): a Change Owner is required to give technical approval for a phase to proceed.
change phase	A stage within a change request. The change phase is the heart of the Change Management (CM) application. The phase identifies the basic components for the system to handle the change through this particular stage of the change process. Every change must have at least one phase defined. approvers can be set for each phase of a change. The next phase in the sequence cannot begin until the previous phase has been closed. A phase can only be closed if all change tasks within the phase have been closed.
change priority	The urgency of the requested change, based on business need.
change queue	The list of changes assigned to an operator, as selected using the operator's default Change Management (CM) inbox.
change record	Records that request, identify, and manage system changes. Each change record has a life cycle typically including approvals, alerts, tasks, phases, and closure. See Request for Change (RFC), Change Management (CM), and Request Management (RM).
change request	A ServiceCenter change ticket. Change requests are the highest level of a change ticket and are created when an element of an organization's infrastructure is to be changed. Change requests are classified by category. A change request does not need to include any change tasks.
change sponsor	In the context of Change Management (CM): a Change Sponsor is required to authorize the change from a customer business perspective. If a Change Sponsor does not have access to ServiceCenter, Change Administrators (cas) are responsible for ensuring that authorization is obtained from the Change Sponsor. A cas must approve the RFC on behalf of the Change Sponsor on the ServiceCenter system.

Term	Definition
change status	Criteria used to define the process of a change through each phase of the RFC management process.
change task	A ServiceCenter task ticket. Tasks look and act very much like change requests. The difference is that a task must belong to a "parent" change request and must have start and end dates that lie within its parent change request's start and end dates. Change tasks are classified by category.
Change Transport System (CTS)	Change Transport System SAP feature that acts as a control mechanism of source modifications to the SAP system.
character delimited	A text file in which values are separated by a character, such as a comma. For example, "alpha, beta, echo, bravo" is comma-delimited.
chart	A graph on a menu or Form that summarizes the status of one area managed by ServiceCenter and the Enterprise Service Desk (ESD), such as changes and tickets.
	See graphs.
CI	See configuration item (CI).
Client menus	The standard menus at the top of the main ServiceCenter Client window: File, Edit, View, Format, Options, List Options, Window, or Help.
Client session	A user interface to the ServiceCenter modules. The client connects to the ServiceCenter application server.
Client window	The main window holding the client menus and all form windows for a single ServiceCenter Client session.
CLOB	Character Large object.
	See BLOB and LOB.
closure	Closure describes the point in time when a call, incident, or root cause has been resolved. Calls are closed at the point where service is no longer required because either the issue is resolved or the call has been escalated to Incident Management (IM). Incidents are closed when the reported issue is corrected, typically when service is restored. Root causes are closed at the point where the underlying issues have been corrected.
CM	See Change Management (CM).
column	The vertical components of a record list or table.
	ServiceCenter files have fields, not columns.
command application	An application designed to run from an operating system command prompt, and therefore designed to be launched by other applications. For example, report.exe, the primary ReportCenter print engine, is a command application.

Term	Definition
command line	A command window available from the ServiceCenter System Administrator's Home menu that lets system administrator's enter ServiceCenter shortcut commands.
command prompt	An operating system user interface prompt where users can launch applications and system functions.
Computer Telephony Integration (CTI)	The software, hardware, and programming necessary to integrate computers and telephones so they can work together seamlessly and intelligently.
configuration	ServiceCenter setup done through the ServiceCenter configuration files (sc.cfg or the CONFIG data set) and initialization files.
configuration item (CI)	A component or item, such as a Request for Change, associated with an infrastructure that is or will be under the control of Inventory Management (ICM). Cis may vary widely in complexity, size, and type. Any object or process within the Information Technology Service Management infrastructure that is recorded in the database, from an entire system (including all hardware, software, and documentation) to a single software module or a minor hardware device.
contact name	A field identifying the user of a component or the main company contact name for items such as, calls, incidents, and requests.
contacts	Those who use components tracked in Inventory Management (ICM) and who contact the Enterprise Service Desk (ESD) to initiate calls, incidents, requests, etc. Contacts should not be confused with operators, who are the personnel using ServiceCenter applications.
contacts file	The ServiceCenter file that contains all contacts records.
contacts record	Information about an individual Contact.
contract	A binding agreement between two parties, tracked and managed by the ServiceCenter Contract Management module.
Contract Management	ServiceCenter module for tracking and managing service contracts through their life cycle.
coordinator	ServiceCenter operator responsible for a call, ticket, or request.
Core	The ServiceCenter Global Knowledge file, which is the default file searched by IR Expert.
CORE	Common object repository.
CSD	Consolidated Service Desk.
CTI	See Computer Telephony Integration (CTI).

Term	Definition
CTS	See Change Transport System (CTS).
cutover	The time when an implementer finishes the primary ServiceCenter implementation and the client begins maintaining ServiceCenter.
Data Definition Language (DDL)	Used for setting up Relational Database Management System (RDBMS) databases and tables.
data policy	A standard ServiceCenter utility used for defining and enforcing overall data rules for individual ServiceCenter files.
database	The repository for all ServiceCenter files. ServiceCenter data resides in a database. Within ServiceCenter, the Database Dictionary (dbDict) defines the field and keys for each file. A file (application file) is a collection of records, each containing values in fields. Each record describes a single entity, such as a location, contact, device, or call. In P4 ServiceCenter's database, the data physically resides in multiple system files, known collectively as the file system. The P4 file system is organized into pools, each containing one or more physical files. When ServiceCenter data is mapped to a Relational Database Management System (RDBMS), each field in each file becomes a column in an RDBMS table. Each ServiceCenter file is mapped to one or more tables in the RDBMS, and each record in the ServiceCenter file is converted to one or more row in the corresponding RDBMS tables.
Database Dictionary (dbdict)	A ServiceCenter utility used to define the fields, keys, location, and overall structure of a ServiceCenter file.
	The ServiceCenter repository that holds all Database Dictionary (dbDict) definitions.
Database Manager (DB)	A ServiceCenter utility used for adding, updating, deleting, viewing, printing, and searching for records in ServiceCenter files.
DB	See Database Manager (DB).
dbdict	See Database Dictionary (dbdict).
DDE	See Dynamic Data Exchange (DDE).
DDL	See Data Definition Language (DDL).
device	Equipment or component, such as a PC or piece of software installed on a PC, tracked through a device record in Inventory Management (ICM).
device file	The ServiceCenter file that contains all device records.
device record	A data record containing details of a piece of equipment or other component.
device type	See type.

Term	Definition
dialog box	A Form in which a user must provide extra information before progressing further.
DLL	See Dynamic Link Library (DLL).
Document Engine	A ServiceCenter utility that lets system administrators define comprehensive processing rules for ServiceCenter files.
drop-down menu	A menu accessed from a field with a designated arrow button (usually pointing downward or to the right).
Dynamic Data Exchange (DDE)	ServiceCenter utilizes Dynamic Data Exchange (DDE) support, so that call lists and incident lists can be exported to an Excel spreadsheet. For example, when the menu option is selected to export to Excel, a spreadsheet is automatically opened and the data is placed in the spreadsheet. The DDE support function requires Excel 95 or later. ServiceCenter DDE support also provides an interface to telephony products to allow you to track telephone calls in ServiceCenter.
Dynamic Link Library (DLL)	A library of executable functions or data, stored in files with a .DLL extension, that can be called by an application.
Enterprise Service Desk (ESD)	An Enterprise Service Desk, includes the individuals, management, processes, tools, and information responsible for responding to issues raised by the user community. In almost all cases, the ESD is responsible for interaction with the user community, particularly the first notification of issues. See service desk and Help desk.
ERP	Enterprise Resource Planning
ESD	See Enterprise Service Desk (ESD).
ESS	Employee Self Service
executables	ServiceCenter run-time environment system programs that run from an operating system command prompt or batch file. This term is typically used in Windows environments.
exit	Exit button that lets you log off or end a ServiceCenter Client session.
false	A logical value equivalent to no or 0.
FAQ	Frequently Asked Questions
FC	See Format Control (FC).
FD	See Forms Designer (FD).

Term	Definition
field	A single data element within a ServiceCenter record. For example, name is a field in the operator file, and its value for one user might be Joe. (A field is equivalent to a column in a Relational Database Management System (RDBMS).)
file	A collection of individual records that share the same Database Dictionary (dbDict) structure. For example, individual device records are contained in the device file. A ServiceCenter file, such as the application file, can reside in a P4 file or can be mapped and converted to one or more equivalent Relational Database Management System (RDBMS) tables.
file system	The physical files that hold all non-Relational Database Management System (RDBMS) data for ServiceCenter implementation. These include P4 system files (whose file names start with scdb.) And IR Expert indexes (whose file names start with ir.).
Fill	The fill function lets a user quickly pull related data into a record, based on a source field and its relation rules defined in a link record. For example, the Fill function can be used to enter a caller's name in the Reported by field in a call record. The caller's full name, phone number, location, and e mail address are automatically filled into the appropriate fields in the call record.
Find	The find function lets a user look up information from a source field. Like the Fill function, Find is controlled by relation rules defined in a link record. With the cursor in a source field, the Find function allows you to directly access the related file. For example, using Find when the cursor is in the Reported by field in a call record accesses the related contacts record, so you can view complete details about the caller.
fixed-width	Text in a file separated by specified fixed character widths, instead of being character-delimited.
Floating Users	Floating Users are defined as user ids that are currently logged onto the system server. Floating Users are allowed into the system, based upon the number of floating seats available in the license pool. A Floating User ID may log onto the system server more than once. Each time that ID is logged onto the system server, running an image of the product, that user will be counted as a Floating User for the applicable system. When the maximum number of Floating Users licensed to a given system have logged on, no further Floating Users can connect to that system. See also Named Users.

Term	Definition
Form	A ServiceCenter GUI screen layout used to access, add, change, and view records in a specific ServiceCenter file, or used as part of the user interaction in a ServiceCenter application. Forms are created and modified using the ServiceCenter Forms Designer (FD) utility.
	Using the Database Manager (DB), a form can be associated with only one ServiceCenter file. However, a file may have many associated forms. Therefore, when you select a file in the DB initial form, you must also identify which form to use, if more than one form is associated with the selected file.
	For example, if you select the location form while running a GUI client, you are accessing the location file using the form location.g. (ServiceCenter automatically determines that you are running a GUI client and provides the .g version of the form, if one is available.) If you select the location file, ServiceCenter presents a list of 21 associated forms for your further selection. All these forms work with the location file, but only one is named location.
	Typically, the primary form associated with a file carries the same name as the file. For example, you use the device (or device.g) form to access the device file. However, forms and files are not identical nor are they synonymous, so care needs to be taken about the looking at the differences between forms and files and when selecting a form.
	See also Format, screen, and Window.
Form window	The window within an overall Client window that displays a Form.
Format	The text-mode equivalent of a Form. Formats are text-mode screen layouts. Forms are GUI-mode screen layouts.
	See also Form, screen, and Window.
Format Control (FC)	An ServiceCenter utility that lets a system administrator build rules to activate behind-the-scenes processing under controlled conditions.
format name	The unique identifying name of a format.
	See also Format.
Forms Designer (FD)	A ServiceCenter utility used to build, modify, copy, rename, and validate GUI Forms to associated files.
framework	A set of integrated service and management processes, tools, work instructions, and service levels used as a platform for the delivery of a consistent productivity center offering.
full name	The complete name of a contact. For example, the contact identified as IRWIN has a full name of Jonathan Irwin.

Term	Definition
function	A built-in ServiceCenter calculation or process. Functions are followed by parentheses that may or may not contain additional parameters. For example, the **tod()** function returns the current system date and time.
GA	See General Availability (GA). See also Managed Availability (MA).
General Availability (GA)	The status of a product and its related document when it is released to the general public.
	See also Managed Availability (MA).
Generic Input Event (GIE)	A ServiceCenter Event Services registration type used to pass Connect.It! data from AssetCenter to ServiceCenter.
	See also Generic Output Event (GOE).
Generic Output Event (GOE)	A ServiceCenter Event Services registration type used to pass Connect.It! data, such as one or more operators assigned to a common area of responsibility, from ServiceCenter to AssetCenter. For example: the assignment groups used in Incident Management (IM) and the Change groups used in Change Management (CM).
	See also Generic Input Event (GIE).
GIE	See Generic Input Event (GIE).
GL	Graphics Language. An SGI Unix application.
GOE	See Generic Output Event (GOE).
graphs	Illustrations (or pictures) used on menus and Forms to plot quantitative information and summarize the status of components, changes, tickets, and so forth.
group	One or more operators assigned to a common area of responsibility. For example, assignment groups are used in Incident Management (IM) and change groups are used in Change Management (CM).
GUI	Graphical User Interface
Help desk	A central support group whose Inventory Management (ICM) primary purpose is to manage, coordinate, and resolve incidents as quickly as possible and to ensure that no request is lost, forgotten, or ignored.
	See service desk and Enterprise Service Desk (ESD).
Hewlett Packard Unix (HPUX)	Hewlett Packard's version of the Unix operating system.
Home menu	The first menu an operator sees after login. Also known as the Main menu.
hot tickets	Incident tickets that have been marked as hot or urgent.

Term	Definition
HPUX	See Hewlett Packard Unix (HPUX).
HTML	Hypertext Markup Language
I/O	See Input/Output (I/O).
ICM	See Inventory Management (ICM).
IM	See Incident Management (IM). See Infrastructure management (IM).
IMAC	When referring to a PC or Laptop system, Install, Move, Change, or Upgrade.
impact category	The business risk of implementing the requested change.
implementation audit log	A record of all the changes made to the base ServiceCenter applications during the implementation process.
Import wizard	A ServiceCenter utility that simplifies importing batch data into ServiceCenter from other applications.
inbox	Inboxes allow you to save queries to conduct pre-defined searches with the same parameters, letting users quickly and easily repeat work queue and other repeated searches. Inboxes are used throughout all ServiceCenter files and records.
incident	The Information Technology Infrastructure Library (ITIL) term for an infrastructure issue that is raised on the Help desk system. The incident is logged by first completing a call record. Any event that requires management beyond the standard operation of the service desk and which causes or may cause an interruption to or reduction in the quality of service. Incidents typically require resolution actions, unlike calls. The difference between a call and an incident is the level of support required for the resolution. This may be based upon the complexity of the issue, number of individuals involved, or amount of work required. Zero, one, or many calls may relate to one incident. It is expected that the resolution of an incident will result in the resolution of related calls.
Incident Management (IM)	The ServiceCenter module for processing incident records through their life cycle, designed to speed and manage identifying, routing, and resolving incidents. Formerly known as Problem Management (PM).
incident queue	The default list of incident tickets of interest to a particular operator; typically, Incident tickets assigned to an operator or to his or her assignment group(s). The list displays, based on the default inbox for this operator.

Term	Definition
incident record	A record opened in Incident Management (IM) after the cause of a reported incident is found. Documentation in the ServiceCenter database, including information the user has reported about the issue, affected item, work history, escalation status, and the resolution actions taken to resolve the issue. Also known as an incident ticket or ticket.
	The two-step close process of an Incident ticket allows the user to break the act of closing a ticket into two steps:
	Resolving a ticket A ticket is resolved when the technician has finished working on it and starts the closing process.
	Inactivating a ticket A ticket is inactivated when the Help desk finished closing the ticket after contacting the customer and confirming the results. Note: It is normal to transfer information from the Call record to the incident record for a particular issue.
incident ticket	See incident record.
Information Technology Infrastructure Library (ITIL)	A set of best practices and processes for managing the support and delivery of IT services. Originally developed for the United Kingdom government in the 1980s, ITIL has become a world-wide de facto standard in the support and delivery of service management.
Information Technology Service Management (ITSM)	The terminology used in Information Technology Infrastructure Library (ITIL) to refer to management of the services provided by an IT department.
Infrastructure management (IM)	Management of behind-the-scenes supporting components, such as the network, phone system, heating, and air-conditioning.
initialization file	A file storing program settings, such as, the sc.ini file, the scstart script, or the PARMS data set, which provides overall configuration and control information. You can edit the sc.ini file manually using a text editor. These files need to be located in the same directory as the command application.
Input/Output (I/O)	On a RIO panel in ServiceCenter, I/O means that users can both enter and view data rather than having just view-only data access.
interfaces and adapters	Software that enables data exchange between applications, such as the SC Auto interface between ServiceCenter and other non-Peregrine applications.
Inventory Management (ICM)	The ServiceCenter module used for tracking components and the relationships between them. Formerly known as Inventory/Configuration Management.
IP	Internet Protocol
IR	Information Retrieval

Term	Definition
IR Expert	IR Expert is an intelligent, concept-based information retrieval (IR) engine that searches the ServiceCenter database for similar/related information, based on a simple, natural language query. For example, instead of relying on exact-match keywords to select like incidents from the ServiceCenter Incident Management (IM) database, the description of an incident is used to locate similar issues, using IR Expert.
IR key	The field in the key is indexed by IR Expert. See keys and key types.
issue	The reason for a support call. An issue may involve a service outage, simple question, or request for assistance or information.
IT	Information Technology
ITIL	See Information Technology Infrastructure Library (ITIL).
ITSM	See Information Technology Service Management (ITSM).
JCL	Job Control Language
JES	See Job Entry Subsystem (JES).
Job Entry Subsystem (JES)	A subsystem of the OS/390 (previously known as MVS) mainframe operating system that manages jobs (units of work) that the system does. The system administrator or other users describe each job to the operating system JCL. The operating system then sends the job to the JES program. The JES program receives the job, performs the job based on priority, and then purges the job from the system.
key types	ServiceCenter uses key types to define key fields in the Database Dictionary (dbDict) of a file. These key fields in turn create indexes, which are used in queries to make searching for records fast and efficient. Key types also assist in maintaining data integrity by controlling the field values in a key. The following ServiceCenter key types are used to allow or disallow certain values across all records within the file for the combined fields that comprise the key: unique no nulls no duplicates nulls and duplicates IR key See keys.
keys	Indexes used for fast searching and data retrieval against ServiceCenter files. See key types.

Term	Definition
kill	A command within the ServiceCenter status monitor to end a process running either a background agent or a user Client session. A ServiceCenter status monitor command to break a ServiceCenter lock.
known error	An incident that is successfully diagnosed with a root cause and for which a temporary work-around or permanent alternative has been identified. If a business case exists, an RFC (Request for Change) is opened in Change Management (CM). A Known Error remains until it is permanently fixed by a change in Change Management.
known error record	A known error record is opened in the Root Cause Analysis module when an underlying problem, or root cause of an incident, has been found. known errors are then used to initiate the Change Management (CM) process.
labor	Work activities recorded against a contract and managed and tracked by ServiceCenter Contract Management.
LAN	See Local Area Network (LAN).
language	The language, such as English, French, or German, selected by a ServiceCenter user. When a user selects a language at login, ServiceCenter Forms are automatically adjusted to that language's default Form width. This is done to accommodate the proportions of different languages. In the basic system, forms in English are widened by 25%. All other languages are widened to 50%. You can adjust this widening further by pressing SHIFT-CTRL+W. This command will widen the form in 25% increments. To narrow the form, press SHIFT-CTRL+N.
life cycle	A series of states, connected by allowable transitions. The life cycle represents an approval process for configuration item (CI)s, Root Cause reports, and Change Management (CM) documents.
line item	A detailed record that identifies a single component or service associated with a quote or order in Request Management.
load library	In OS/390, run-time environment programs that run from the JCL or as a started task.
LOB	Large object. See BLOB and CLOB.
Local Area Network (LAN)	The connection of multiple computers within a building, so that they can share information, applications, and peripherals. See also Wide Area Network (WAN).
localization	Configuring an application so it runs correctly in a local environment. This includes, but is not limited to, language-specific Forms, messages, help, and appropriate date formats and currency.

Term	Definition
location file	The file that contains all the location records, used in many ServiceCenter modules.
location record	Details of a single location.
Log In	To start (the act of starting) a an individual ServiceCenter Client session by entering a ServiceCenter login name and password that match values in an existing ServiceCenter operator record. See login.
log out	To end (the act of ending) an individual ServiceCenter Client session. This is different from a server shutdown. See Logout.
logical	A ServiceCenter data type used to hold a value of true, false, unknown, or null, or to hold an expression that evaluates to one of the above-mentioned values.
logical name	A field that uniquely identifies each device. For example, Jonathan Irwin's PC has a logical name of pc001.
login	The name a user logs in with. The process of starting an individual ServiceCenter Client session. See Log In.
Logout	The process of ending an individual ServiceCenter Client session. The end of a user session. See log out.
MA	See Managed Availability (MA). See also General Availability (GA).
mail	Internal ServiceCenter mail, stored in the ServiceCenter mail file. This is different from standard external e-mail managed through MAPI or SMTP.
Main menu	The first menu an operator sees after login. Also known as the Home menu.
Managed Availability (MA)	The status of a product and its related document when it is released to a few select customers only. See also General Availability (GA).
manager	Person in charge of overseeing a project to completion.
MAPI	Messaging Application Programming Interface
marquee	A scrolling message bar that a system administrator can add to any Form or menu by selecting the marquee widget (tool) in the Forms Designer (FD).

Term	Definition
maximum resolution	Time frame within which all incidents should be resolved. This is a worst case SLA and should not be used to drive the allocation of resources by the SDU.
MDI	See Multi-Document Interface (MDI).
menu	A ServiceCenter Form containing buttons that launch ServiceCenter applications, including other menus.
message	A ServiceCenter notification. See notification.
MIB	Management Information Base Related to SNMP.
minimum resolution	The minimum level of SLA achievement to be delivered. Failure to meet this measure will cause service penalties to accrue.
MIS	Management Information Systems
mobile user	Users that are dependent upon a mobile computer system to perform their normal business function and not usually able to attend a client location to receive support.
model file	The file that contains details of all models tracked in ServiceCenter. Each model record tracks details (such as model number, manufacturer, and ordering information) for a particular type of component or system from a particular manufacturer.
module	A major ServiceCenter application. These include: Change Management (CM) Incident Management (IM) Inventory Management (ICM) Scheduled Maintenance Service Management (SM) Service Level Agreement Root Cause Analysis (RCA) Work Management (WM)
Multi-Document Interface (MDI)	The standard ServiceCenter GUI structure with a main Client window, containing Client menus at the top (File, Edit, and Help) and one or more Form windows.
MVS	A mainframe operating system. Later versions are called OS/390.

Term	Definition
Named Users	Named Users are unique users that are authorized to log onto ServiceCenter under a different status than Floating Users. Named Users are allowed to log onto ServiceCenter at any time, based on their authorization code and license agreement with Peregrine Systems. Their seats are reserved in ServiceCenter and are always available for login. If a Named User logs on multiple times at the same work station, the system only uses one license seat. If a Named User logs on to multiple work stations, the Named User license is used at the first login, then each subsequent login takes a floating license seat. See also Floating Users.
network	The physical and logical connections between the devices in a business. A network in one location is referred to as a Local Area Network (LAN). A dispersed network is referred to as a Wide Area Network (WAN).
network address	The unique identifier for a device on a network, such as a PC. For example, the IP address is often used. An IP address contains four sets of numbers, joined by periods (for example, 111.22.333.44).
network name	The name of the network or network segment where a device resides. For example, the Peregrine Systems main network could be called Peregrine Main.
Network Node Manager (NNM)	The primary module within HP Openview.
NFS	Network File System
NNM	See Network Node Manager (NNM).
no duplicates	A type of ServiceCenter key. The value in the field or combination of fields in the key must not be the same as any other field. See keys and key types.
no nulls	A type of ServiceCenter key. At least one field in the key must not be null (empty or missing). See keys and key types.
notification	A ServiceCenter message delivered in an on-screen Active Note, the Form window window's status bar, or the ServiceCenter mail file. Also a message sent externally, using email, pager, or fax.
NSM	Network and Systems Management

Term	Definition
nulls and duplicates	A type of ServiceCenter key. All fields can be null (empty or missing), and the complete key can be duplicated in the index.
	Both null (empty or missing) values and duplicate values are allowed across all records within the file for the combined fields that comprise the key.
	See keys and key types.
number file	A ServiceCenter control file that holds the last number used for system-assigned tracking numbers (for example, incident ticket numbers, change requests, and model numbers).
OBID	OBject ID
Object Linking and Embedding (OLE)	Technology for associating external files with ServiceCenter records, replaced in ServiceCenter 4.0 and later by file attachments.
OCI	See Oracle Call Interface (OCI).
OCM	Order and Catalog Management
ODBC	See Open Database Connectivity (ODBC).
OK	A commonly-used button within ServiceCenter that saves the record currently displayed on the screen, then exits the current Form and returns to the previous menu or form.
OLAP	See Online Analytical Processing (OLAP).
OLE	See Object Linking and Embedding (OLE).
Open Database Connectivity (ODBC)	A Microsoft-developed set of database access APIs. All data access requests to an ODBC driver use the same set of low level calls and protocols within the ODBC API. It is the role of the ODBC driver to translate these calls into instructions that are specific to a particular Relational Database Management System (RDBMS). The advantage of using ODBC as a data access layer is that the same client application, such as ReportCenter, can access multiple, dissimilar database servers (for example, Oracle, Sybase, and Informix) without requiring a separate version for each. The application makes the same calls to the ODBC driver, which then translates them into vendor-specific database calls.
operator	Users who log on to ServiceCenter. This is normally a smaller group than the contacts who use the devices, software, and services that ServiceCenter supports.
	See also contacts.

Term	Definition
operator file	A file containing details of all users who log on to ServiceCenter, including the login name and password, company, full name, Home menu, capability words, and the user's default printer, time zone, date formatting and currency.
operator record	The details of one ServiceCenter user, stored in the operator file.
Option	A selection from the Options menu.
Oracle Call Interface (OCI)	The primary tool used to communicate between ServiceCenter and Oracle in ServiceCenter 3.0 SP3 and later.
order	A record generated when a Request Management quote has been approved and is ready for ordering. One quote can generate one order or multiple orders. Each order can have no line items, one line item, or many line items.
OS/390	A mainframe operating system. Earlier versions are called MVS.
P4	The proprietary Peregrine flat-file database used to store ServiceCenter data. It can be replaced with any ServiceCenter-supported Relational Database Management System (RDBMS).
page	An individual history record in a set of common records. For example, each time a request for change (RFC) is updated, a new page can be written if this option is turned on for the change phase. The new page then becomes part of the RFC's history.
parameter	A control setting passed to a ServiceCenter function, service, or Rapid Application Development (RAD) application in an initialization file or on a command prompt.
parts	Components tracked against a contract within Contract Management.
password	An encrypted authentication code used during ServiceCenter login.
PDA	Personal Digital Assistant
Peregrine Repository Interface Manager (PRIM)	PRIM has been largely replaced by Connect.It! in ServiceCenter 4.
phase	Administrative steps within a change, quote, or order. Phases are sequential, repeatable steps characteristic of a change, quote, or order category. You can approve, complete, cancel, or close a phase. After taking action on a phase, you can move to the next phase. Each phase can include none, one or more tasks. When all tasks for a given phase are complete, the phase is complete (and cannot be closed until the tasks are closed). When no more phases exist for an item (change, quote, or order), then the item can be closed.

Term	Definition
physical file	A P4 system file. This is a Unix or Windows NT file, or an OS/ 390 data set, recognizable by the operating system residing in a directory on a drive. One ServiceCenter physical file can contain many application files, as defined within the ServiceCenter Database Dictionary (dbDict). Each ServiceCenter pool resides in one or more physical files. ServiceCenter 4.0 supports up to 75 physical files.
PID	See Process Identification (PID).
pool	A logical data collection. In P4, all data is stored in pools. All files, such as application files defined by a Database Dictionary (dbDict) record, belong to a pool (pool 3 by default). ServiceCenter uses other pools to track indexes, free lists, and associator records.
pop-up menu	A menu accessed by pressing the second or third mouse button. This menu is not part of the menu bar.
pop-up window	Temporary dialog box that displays either a message or a prompt.
PRIM	See Peregrine Repository Interface Manager (PRIM).
priority	Sequence in which a Root Cause or Change needs to be resolved, based on impact and urgency.
Probable Cause	Predefined description of the cause of a call or incident. Tickets contain an optional Cause Code field that links the ticket to a Probable Cause record. When a cause code is added to a ticket using the Fill function, accompanying information, such as the default category and description, also fills into the ticket from the corresponding Probable Cause record. ServiceCenter ships with a probcause file containing sample Probable Cause records. See also cause code.
problem	Now known as incident.
Problem Management (PM)	Now known as Incident Management (IM).
process	A connected series of actions, activities, changes, etc. performed by agents with the intent of satisfying a purpose or achieving a goal. An instance of a program running on a computer. For ServiceCenter, this is either a user Client session or a background agent.
Process Identification (PID)	A unique identifying number for each process running on a machine.
profile	A security record that defines the Options and authorities available to the operator or group using the profile.

Term	Definition
prompt	A dialog box that appears at strategic points, giving the user a choice of actions (for example, yes, no, OK, and cancel).
QBE	See Query-by-Example (QBE).
Query-by-Example (QBE)	A file search, using values entered on screen. If multiple records match the search parameters, a QBE list (also known as a record list) displays from which you can select the record you want to view.
quote	A request within the ServiceCenter Request Management application. One quote can contain many line items, collectively identifying the goods and services a user is requesting. Once approved, one quote can generate one or more related orders.
RAD	See Rapid Application Development (RAD).
RAD debugger	A tool for troubleshooting Rapid Application Development (RAD) processes in ServiceCenter.
RAID	Redundant Array of Inexpensive Disks.
Rapid Application Development (RAD)	A programming method that uses a series of panels to create and run ServiceCenter applications and utilities.
RC	See ReportCenter (RC).
RCA	See Root Cause Analysis (RCA).
RDBMS	See Relational Database Management System (RDBMS).
record	Set of data fields contained in a file, that describes a single entity (for example, a device, ticket, location, or contact). An entry in a file is roughly equivalent to a row in an RDBMS table. See also Relational Database Management System (RDBMS).
record list	ServiceCenter view that combines a Query-by-Example (QBE) list in the top part of a Form window, a Form below displaying a single record from the list, and a split bar separating both forms.
refresh rate	See automatic refresh rate.
registration	In the context of Inventory Management (ICM), the method of identifying and recording an object or entity.
Relational Database Management System (RDBMS)	Any of several databases used to store ServiceCenter data if P4 is not used.
relationships	In the context of Inventory Management (ICM), the connectivity, link, and/or dependency between two or more configuration item (CI)s.

Term	Definition
Report engine	A collection of Seagate DLLs and supporting files used by ReportCenter to print report files created using Crystal Reports. The report engine must be installed on each user's machine for ReportCenter to work.
ReportCenter (RC)	The Windows-based application that enables users to generate graphical reports, using ServiceCenter data.
reports	Files with the RPT extension which are either shipped with ReportCenter or created using Crystal Reports.
	Reports created with the ServiceCenter Report Writer utility, either shipped with ServiceCenter or created using the Report Writer.
	User-created output, summarized or detailed, created with any reporting tool.
repository	The database or container for all ServiceCenter data. This includes the file system for P4 only.
request	See Request for Change (RFC).
Request for Change (RFC)	A Form used to record details.
	A request for a change to any configuration item (CI) within an infrastructure or to procedures and items associated with the infrastructure.
	A standard change request category shipped with ServiceCenter 4.0 and later. A change record is opened when a change to the IT infrastructure is needed to prevent further failures of configuration item (CI)s.
	See Request Management (RM).
Request Management (RM)	The ServiceCenter module for processing Request for Change (RFC)s and their related change record through their life cycle. A change record is opened when a change to the IT infrastructure is needed to prevent further failures of configuration item (CI)s.
reserved words	Terms or words that have been set aside for exclusive use within Rapid Application Development (RAD) programming, queries, or system tailoring.
resolution	An action which will solve an incident. This may also be a work-around.
resolution teams	Level two and higher technicians: the individuals, management, processes, tools, and information responsible for resolving issues. In some cases, the Enterprise Service Desk (ESD) technicians are able to resolve the reported issues reported in a call. In many other cases, however, the issue needs to be escalated to the appropriate resolution team.
response time	The time required to change an incident ticket from one status to another (for example, from Open to Resolved).

Term	Definition
reviewers	Personnel who can examine the tasks and phases of a Change Management (CM) change, but who do not have approval authority.
RFC	See Request for Change (RFC).
RIO	Record Input/Output See also Input/Output (I/O).
Risk	A measure of the exposure to which an organization may be subjected. This is a combination of the likelihood of a business disruption occurring and the possible loss that may result from such business disruption.
RM	See Request Management (RM)
role	A set of responsibilities, activities, and authorizations.
root cause	An issue that is causing other issues. A root cause will always require further assessment and will generally require resolution. Zero, one, or many incidents may be associated with a root cause. Calls are not normally associated with root causes. See also Root Cause Analysis (RCA).
Root Cause Analysis (RCA)	The ServiceCenter module where an incident that cannot be resolved by the Service Desk Analyst (SDA), is passed to a Service Delivery Unit (SDU) for resolution. The associated call record, if one exists, is linked to it to facilitate monitoring, tracking, and analysis.
root cause record	The documentation in the ServiceCenter database of the information the user reports about an issue, combined with the research details about the underlying issue. Data may be copied from an incident record to a root cause record.
row	A collection of data (column) that describes a single entity in a Relational Database Management System (RDBMS) table.
RTE	See Run-Time Environment (RTE).
Run-Time Environment (RTE)	The binary, load library, or executable layers of ServiceCenter containing server and client code.
SAP	See Selective Alternative Process (SAP).
save	Keep the updates made in a record. Revisions can be saved manually or automatically. See also autosaving.
SC Auto	See ServiceCenter Automated (SCAuto).
SC Distributed	See ServiceCenter Distributed (SCD).

Term	Definition
SCAuto	See ServiceCenter Automated (SCAuto).
SCD	See ServiceCenter Distributed (SCD).
Scheduled Maintenance	A ServiceCenter module for scheduling, completing, and tracking routinely recurring activities on different components and device types in different locations.
SCM	Supply Chain Management
screen	See Form, Format, and Window.
SDA	Service Desk Analyst
SDK	See Software Development Kit (SDK).
SDU	See Service Delivery Unit (SDU).
search	The process of trying to locate a ServiceCenter record(s). See Query-by-Example (QBE).
Selective Alternative Process (SAP)	An enterprise resource planning application that includes manufacturing, distribution, finance, and human resources modules.
server	The computer that hosts a server application, such as the ServiceCenter server, a database server, or a print server. The server software portion of a client/server application.
service	A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.
Service Delivery Unit (SDU)	A support group responsible for resolving incidents appropriate to the skills of the unit.
service desk	The single point of contact within the IT organization for users of IT services. See Help desk and Enterprise Service Desk (ESD).
service information	Service agreement data, including contractor, agreement number, serial number, model, service hours, installation and warranty dates, procedures, pricing, and response information.
service level	The expression of an aspect of a service in definitive and quantifiable terms; specifies a term in an SLA and quantifies its associated measures.
Service Level Agreement	A contract with a company or department for maintaining and repairing equipment or providing other services.
Service Level Management (SLM)	The ServiceCenter module for tracking and managing Service Level Agreements.

Term	Definition
service maintenance objective	The maximum time that an IT component remains unavailable before service is restore.
Service Management (SM)	In Information Technology Infrastructure Library (ITIL), the management of services to meet the customer's requirements.
	The ServiceCenter module for the management of services to meet the customer's requirements. The Service Management module to processes call records through their life cycle. The module is also responsible for defining the relationships between calls and incidents.
service provider	A third-party vendor/organization supplying services or products to customers, for example, the telephone company.
ServiceCenter Automated (SCAuto)	The base product for asynchronous interfaces that manage near-real-time data exchange between ServiceCenter and other applications.
ServiceCenter Distributed (SCD)	In order for each site to share its data with other sites in the network, SC Distributed makes sure that updates at any site are propagated to all sites that have a copy of an incident ticket. Even though each site has its own files and tickets, those tickets can be assigned to or shared with other sites. SC Distributed makes sure that updates at any site are propagated to all sites that have a copy of an Incident ticket.
Serviceinfo client	A special client that does not count against an installation's ServiceCenter licensing. It displays view-only Forms with charts and marquees.
session	See Client session.
Simple Mail Transport Protocol (SMTP)	The TCP/IP email protocol.
site category	Used to define the size of a site or campus location by number of users, which would alter the way the site is supported and on-site resources are allocated.
SLA monitoring	A chart used to monitor the compliance of the Service Level Agreement.
SLM	See Service Level Management (SLM).
SM	See Service Management (SM).
SMTP	See Simple Mail Transport Protocol (SMTP).
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
Software Development Kit (SDK)	The kit used to build custom ServiceCenter Automated (SCAuto) interfaces.

Term	Definition
SQL	See Structured Query Language (SQL).
SQL views	SQL select statement that can be treated like a table. These can be used to limit access to certain sections of data, remap a database schema that has been modified, or include calculated fields at the database level.
state	A concept used in the Document Engine in ServiceCenter 4.0 and later. Regardless of the module, an object, such as cm3profile, is referenced whenever a Form is opened and determines the behavior for the state of the form (for example, open, list, or search).
statement of work	A detailed document that describes the work that will be completed during a ServiceCenter implementation.
status	The current state of a record or device.
Status bar	The bottom portion of a ServiceCenter window, which displays messages, status data, and the current Form name.
string operator	Also referred to as the concatenation operator. Arranges strings of characters into a chained list.
Structured Query Language (SQL)	A standard interactive and programming language for getting data to and from a Relational Database Management System (RDBMS).
system administrator	A ServiceCenter user with sysadmin privileges who is in charge of maintaining the system.
system language	The vocabulary that ServiceCenter uses to communicate internally with its various routines and processes and to interact externally with its users.
system tray	The section of a Form window below the toolbar that contains context-sensitive buttons, such as Back, OK, Save, Find, Fill, Logout, and Command.
table	A collection of rows in a Relational Database Management System (RDBMS). See database for more background. ServiceCenter has only files, not tables, although a ServiceCenter file can be mapped and converted to one or more RDBMS tables. Forms Designer (FD) object with multiple rows and column.
Table Designer	Now referred to as the Database Dictionary (dbDict) utility.
tabs	A Forms Designer (FD) object that provides overlapping areas with different information on a single Form. Users click the desired tab to move it visually in front of all the other tabs to access the fields.

Term	Definition
tailoring	Changes made to ServiceCenter by creating and modifying control records, using ServiceCenter utilities. Tailoring is the normal method of adapting ServiceCenter to each installation's requirements. Tailoring involves no Rapid Application Development (RAD) programming or coding changes.
target achievement	A Service Level Agreement achievement targeted to be delivered. See Service Level Agreement.
task	A work process that has been designated as necessary for a Change Management (CM) Request for Change (RFC) or the phase of a change request. For example, an RFC requesting replacement of a hard drive with a larger model might involve several tasks, including ordering the new drive, backing up the old drive, and installing the new drive.
task category	Classification of the task in a requested change. The category determines the data to be collected for a particular task, Forms to be presented to the user for data entry, approvals needed, and intervals at which alerts will be sent. ServiceCenter includes a series of default categories. System administrators can create new categories.
task list	List of tasks, based on an inbox.
task number	Unique number assigned to a task.
task phase	A sequential step within a task. See also phase.
task queue	The task list (inbox) for a technician.
TCO	Total Cost of Ownership.
TCP	Transmission Control Protocol
TEC	Tivoli Enterprise Console
technician	A person who does the work and performs the tasks associated with ServiceCenter incidents, changes, and requests.
Time Sharing Option (TSO)	In the context of OS/390, a subsystem that lets a terminal user's session invoke OS/390 facilities interactively.
trace	A debugging function that allows the user to see the panels encountered by the Rapid Application Development (RAD) flow. See also RAD debugger.

Term	Definition
trigger	An automated database activity defined by a rule in the trigger file and activated by a related activity in a ServiceCenter file. For example, when a user updates an incident ticket, the related probsummary record is automatically updated in accordance with rules defined in a trigger record.
true	A logical value equivalent to yes or 1.
TSO	See Time Sharing Option (TSO).
type	A broad classification for devices. Also known as device type.
UCS	See Universal Character Set (UCS).
unique	A type of ServiceCenter key. Each record's combined values for the fields comprising the key are different from any other record within the same file. At least one field in the key must not be null (empty or missing), and the value of the complete key must be unique in the index. See keys and key types.
Universal Character Set (UCS)	In the context of IBM, used on the 3800 printing subsystem on the data definition (DD) statement or output statement in the JCL. Specifies the one to four character name of the print band to be used to print the data set.
update	Modify an existing record in a ServiceCenter file.
user authentication	Set of requirements to prove the identity of a caller before completing changes to data security access.
User Role	A field in the operator record that contains information on a number of user roles. When a role is selected, the application profiles for the operator record will be populated according to the information bundled within that particular User Role.
users	Personnel using ServiceCenter to do their jobs. Also known as operator. Personnel supported by the people using ServiceCenter. Also known as end users or contacts.
Utility	ServiceCenter administrative tool typically used in setup or maintenance of multiple ServiceCenter modules, rather than performing module-specific tailoring.
value	The entry for one field on one Form or in one record.
variable	A value that resides only in memory, disassociated with any record and not stored in the ServiceCenter database.

Term	Definition
vendor	A manufacturer, supply source, or service contractor stored in the ServiceCenter vendor file.
vendor file	A ServiceCenter file containing records of vendors, manufacturers, and service contractors for your organization.
Virtual Telecommunication Access Method (VTAM)	Provides centralized control over devices attached to an OS/390 system.
VTAM	See Virtual Telecommunication Access Method (VTAM).
WAN	See Wide Area Network (WAN).
Wide Area Network (WAN)	The connection of multiple computers located at two or more physical sites, normally using digital data circuits.
Window	See Form, Format, and screen.
WM	See Work Management (WM).
Work Management (WM)	A ServiceCenter module for graphically viewing and optimizing technicians' work schedules.
work-around	Method of avoiding an issue or incident, either from a temporary fix or by not relying on the particular item known to have a problem.
XML	Extensible Markup Language.

Index

Symbols
(AG) 138

A
Access Control List 137
ACL 137
Active Notes 137
activity type 137
add 137
administrative privileges 137
administrator 138
Advanced Interactive Executive 138
affected hardware 138
AG 138
agents 130
AIX 138
alert status 138
alerts 138
API 138
Application Generator 138
application layer 14
application profiles 29
application suite 138
applications 138
approval 138
approval group 138
approval sequence 138
approver 139
architecture 14
asset 139
AssetCenter 19

assignment group 139
associate 139
attachment 139
attribute file 139
attributes 139
audit specifications 130
Automation suite 18
autosaving 139
availability 139

B
background agent 140
background scheduler 140
best practice steps
    Inventory Management 93–103
binaries 140
BLOB 140
broadcasting messages 130
browse 140
btree 140
build 140
button 140

C
CA 140
CAB 141
CAB/EC 141
Calendar 140
call 140
call record 140
call report 141