SERENA®

SERVICE MANAGER

User's Guide

Serena Proprietary and Confidential Information

Trademarks

U.S. Government Rights

Table of Contents

Chapter 1: What's New in this Release?

The following features and changes are new in Serena Service Manager and Serena Request Center.

- Service Level Agreements [page 7]

- Request Fulfillment Workflows [page 7]

- Dynamic Forms [page 8]

- Enhanced Social IT [page 8]

- Starter Pack [page 8]

- Miscellaneous Serena Request Center Improvements [page 8]

- Serena Release Manager Integration [page 9]

Service Level Agreements

Service Level Agreements (SLAs) define the level of service that an organization commits to its customers. You can now configure the SLA feature in SBM Application Administrator to define metrics for tracking these commitments. SLAs can be tailored to specific customer requirements. For example, incidents in the "Classification" state must reach the "Closed" state within 12 hours if the value of the *Priority* field is "1."

Users have distinct reasons to monitor SLAs. Technicians need to know about SLAs that apply to their items so they can prioritize their work. Managers need historical information to measure how well their organizations conformed to SLAs and forecast information to ensure that active items are not in danger of violating SLAs. SLA metrics are accessible to users through SLA reports and forms in the SBM User Workspace. Notifications can be sent to users to alert them when violations occur or items are at risk.

Request Fulfillment Workflows

The Incident Management process app has been renamed to Service Desk Process App and includes three new workflows under **Service Requests**. These workflows can be used for your request services, and they are used by the Starter Pack Services.

The new Request Fulfillment workflows are:

- **Atomic** - This workflow is used for requests that require a business approval but not a financial approval.

- **Requisition** - This workflow is used for requests that require financial approval but not business approval.

- **Composite** - This workflow is designed for requests that require subtasks in other applications to be completed.

Dynamic Forms

The transition and state forms in Service Manager have been redesigned using the new form actions feature available in SBM Composer. Form actions became available with Serena Business Manager 10.1, and they allow for dynamic customization of forms based on events and actions. For example, if a user selects a certain value in one field, a related field is either added to or removed from the form. Form actions eliminate much of the JavaScript used on the forms in previous releases.

In addition, the use of form actions in Serena Service Manager 3.0 has drastically decreased the number of forms needed for each process app. Instead of using custom forms for each state and transition, a limited number of forms with form actions are required and they can provide the same benefits.

For more information on form actions, see *SBM Composer Guide*.

Enhanced Social IT

Service Desk Process App includes the Social IT feature, which was introdcued in Serena Business Manager 10.1. The **Social Widget** is added to forms in the Service Desk Process App.

The widget displays data for all users who have interacted with specific items. Users' avatars display, along with their contact information. By expanding a user's entry, you can see additional details such as the number of item updates, associated emails, and transitions performed. You can also use the Suggest Expert functionality to view users who have worked on similar issues.

Starter Pack

The Starter Pack is included with the Serena Request Center. After importing and deploying the components included in the Starter Pack, your Request Center is ready for immediate use. The starter pack includes:

- Service Desk Process App, which includes Incident Management and Request Fulfillment workflows.

- Starter Pack Services, which are predefined services in Request Center. Each service has an accompanying project created within the Service Desk Process App.

- Starter Pack Forms, which are tailored submit and state forms for the different services.

  Note: Starter Pack Forms makes use of external forms, which were introduced in Serena Business Manager 10.1. External forms are located in one process app but are based on a primary table in another process app. Starter Pack Forms reference the Service Desk Process App and the external forms are chosen as the Submit form for the predefined Starter Pack Services.

For more information, see Chapter 3: Serena Request Center [page 21].

Miscellaneous Serena Request Center Improvements

- Serena Request Center's look and feel has been changed.

- Administrators can now choose a display order for categories and services. This allows administrators to sort categories and services based on importance, instead of only alphabetically.

- Projects and services now require a one-to-one relationship. SRC administrators will see alert icons 🔴 for the services that do not meet that requirement.

- The **Query at Runtime** option in the project drop-down is no longer allowed, due to the preceding restriction of a one-to-one relationship between services and projects.

- Links to open and create projects in SBM Application Administrator.

- Display of SLA title and description for the selected project.

- Ability to select a different **Submit** form than the one specified in the workflow. This means that the default Submit form for the project can be overridden by the service.

Serena Release Manager Integration

Service Manager includes changes to the Change Management process app to integrate with Serena® Release Manager (SRM). The additional transitions and forms allow users to link and unlink release trains to change requests.

For more information, see Integration to Serena Release Manager [page 91].

Chapter 2: Welcome to Serena Service Manager

This chapter gives an overview of the pieces included with Serena Service Manager and Serena Request Center.

> **Note:** If you purchased Serena Request Center, you will receive a subset of the pieces that are included with Serena Service Manager. Serena Request Center includes Service Desk Process App, Starter Pack Forms, Knowledge Management, and SRC. The ITSM process apps such as Problem Management, Change Management, and Configuration Management System are only included if you purchased Serena Service Manager.

Serena Service Manager

Serena Service Manager is a process-driven approach to ITSM – one that allows business and IT to work together, in perfect harmony. Unlike traditional ITSM solutions that are difficult to use, expensive to maintain, and provide limited visibility across the service delivery lifecycle, Serena Service Manager draws on the power of a process management platform at its core to provide you with the following benefits:

- Lowers TCO

- Complete visibility

- Improved user satisfaction and agent productivity

- A contemporary interface for IT services

Serena Service Manager comes packaged with fully functional, easy-to-use applications including those for Request, Incident, Problem, Change and Configuration Management.

Service Manager also provides the IT operations team with visual dashboards and robust report generation capabilities so that they can maintain complete visibility across the end-to-end service delivery process. This includes the ability to view actionable metrics related to costs and resource utilization.

Serena Request Center

Serena Request Center provides a one-stop interface for corporate users to discover and request IT services, submit incidents, and review knowledge base articles. It comes with a rich, interactive, and intuitive web portal. The portal contains an enterprise service catalog allowing for services to be composed, organized and published into convenient categories for anytime, anywhere access.

The portal comes pre-populated with IT Services use the request fulfillment workflows in the Service Desk Process App, such as New Hire and Install OS. The services also make use of the Starter Pack Forms, which are customized external forms for submitting requests.

Service Manager Process Apps Overview

The Serena Service Manager is composed of the following process components:

- **Request Fulfillment**, which addresses service requests from users by providing a request channel, gathering or supplying information, and fulfilling the request. (This is part of the Service Desk Process App and included in SRC.)

- **Incident Management**, which focuses on restoring normal service operations as quickly as possible to minimize the impact of incidents on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. (This is part of the Service Desk Process App and included in SRC.)

- **Problem Management**, which analyzes the root cause of incidents, prevents their recurrence, and limits the impact of problems that cannot be prevented. Problem management includes the **Workarounds** auxiliary table, where information on workarounds is stored.

- **Change Management**, which helps ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure. This minimizes the number and impact of any related incidents upon service after changes are implemented.

- **Configuration Management System (CMS)**, which oversees the life of the Configuration Items (CIs) through enabling the fundamental elements of identification, change management, status accounting, and audits. The CMS is composed of three pieces, the **CMS** where all CIs are stored, the **CMS Baselines** workflow where all of the CI baselines are processed, and the **Relationships** auxiliary table where the relationships between CIs, RFCs, Problems, and Incidents are stored.

Here is a graphical representation of the different process components and how they work together:
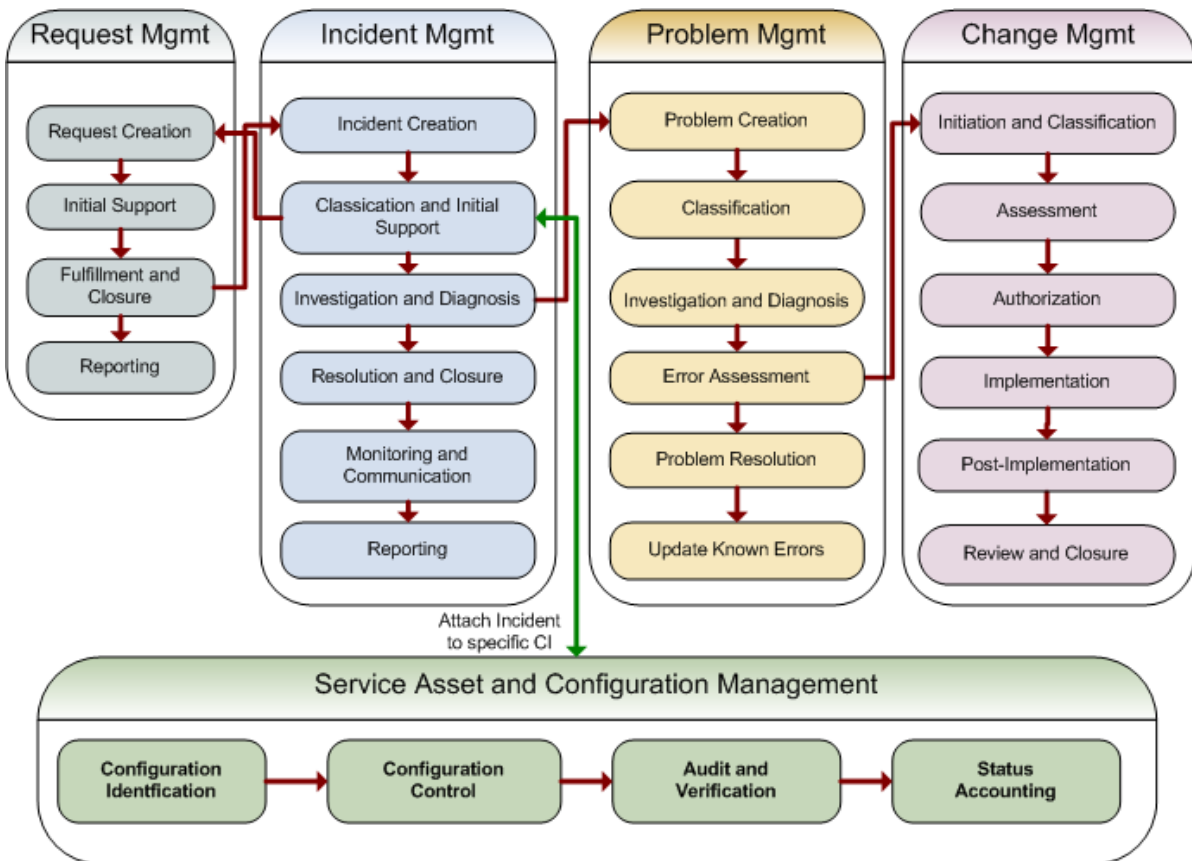
A typical integration flow is as follows:

1. *Configuration Items (CI)* are entered in the Configuration Management System and stored in the CMS. Baselines of CIs are stored in the CMS Baselines project.

2. End users or Service Desk staff submit an *incident*, choosing the **Affected CI** for the incident, which creates a link between the incident and the CI.

3. If the incident needs to be escalated for root cause analysis, a *problem* is submitted based on the incident.

4. Problems can lead to entries in the *Known Errors* table, documenting workarounds for problems, and resolutions to Known Errors.

5. Problems can lead to the creation of a Request for Change (RFC), which is formal proposal for a change to the IT infrastructure.

6. An RFC may require an update to a CI and a new CI baseline.

General Features

The following topics describe the general features and settings available in the Serena Service Manager.

These features apply to all of the processes: CMS, Incident Management, Problem Management, and Change Management. For information on specific process apps, refer to Chapter 11: Additional Information [page 117].

Role Based Access

For each management process, administrators can map functional and access privileges to users by assigning the appropriate roles.

Access to items and data are controlled by roles. Roles can grant read-only access to one group and update privileges to another. Data attributes can also be classified, and access to each data classification granted by role.

Functional privileges include access and ownership over the workflow. The ability to transition problems from one state to another is also controlled by the role privileges. Furthermore, owners are assigned to each active state in a workflow.

Roles are customizable, allowing you to tailor the roles to your installation.

Workflow Rules

Workflow rules determine how an item should progress through the workflow, and if certain criteria must be met before an action can be performed. These actions can be performed automatically.

For example, workflow rules can be established to ensure that a CI has valid data. If these conditions are not met, an automated action can be launched on the item, such as preventing the item from being transitioned to the next state.

Service Level Agreement Compliance

A Service Level Agreement defines the level of service that an organization commits to its customers. Projects can be associated with a specific Service Level Agreement, allowing you to track SLA compliance for items submitted in that project.

The SLA widget displays the status of the current SLAs that pertain to that item. The SLA widget is included on state forms for both Incident Management and Service Requests.

Tip: You can add the SLA widget to your custom state forms using SBM Composer.

SLA reports are available to managers who can access historical information to measure how well your organization conformed to SLAs and forecast information to ensure that active items are not in danger of violating them.

Audit Trails

Serena Service Manager includes the complete tracking functionality of SBM, which enables you to track changes to every item. Each item is assigned a unique identifier after it is created in Serena Service Manager. Every activity is recorded, including field updates, transitions, and relationships, as the item moves through the workflow.

You can access this information through viewing the Change History of the item or from running reports to gather information about the item. This data provides an audit trail for the item throughout its lifecycle, and you can use this data to improve your processes.

Auxiliary Tables

Multiple auxiliary tables are included which contain values that are used by selection fields. The values for these fields can be easily modified from SBM User Workspace by modifying the auxiliary tables.

State Forms

State forms are displayed when an item is in a state. They are designed with the following features to give visual indicators of the status of the item and of the important information.

1. The state icon gives users a visual cue of where the item is in the workflow. The icon is added during form load using a form action. The colored backgrounds are based on the process app that you are in.

2. Primary transition buttons are enlarged to display to users the usual path through the workflow. Secondary transitions and item actions, such as **Update** and **Send E-mail**, are collapsed to reduce the clutter on the page. Expand to access

3. Service Level Agreement status appears on the left side. It displays the current SLA status for the highest SLA pertaining to the item. Click on the SLA widget to display details about the Service Level Agreement and to display other service level agreements that are related to the item.

4. The item's title appears along the top of the item.

5. Working group **Social** widget displays users who have interacted with the item.

Transition Forms

Transition forms are displayed when you click a transition button on the state form or submit a new item. Transition forms share a similar layout, which assists you when populating the form with the necessary information.

1. Required fields are highlighted in yellow calling attention to fields that must be populated. This is done by adding background coloring to the cells for the form in SBM Composer.

2. Relational fields enable a keyword search with a drop-down list of results.

3. **OK** and **Cancel** buttons are placed on the bottom of the form.

    Note: For form designers: the forms are designed so that fields that are set automatically are put into the System section of the form. Other fields are in the User section so that users will be able to view the fields that require information. In addition, form actions are used for modifying the form design such as setting the transition icon on page load.

Working Groups and Suggested Experts Panel

Custom forms may include the **Social Widget**, which displays the working groups and the expert panel where you can select to have experts suggested for the item.

Working Group

The working group shows the number of interactions other users have had with the item and then displays the number of interactions for each of those users. It also displays the current fields where the user is selected. The users are sorted based on the number of interactions in a list. You can click 💬 to send an email to that user.

The current user is not displayed in the list of users in the working group.

You can select a user in the list to display the details pane. The details pane contains contact information for the user, the number of interactions broken down by type, and the current fields where the user is selected, such as **Owner** or **Submitter**.

The interactions are divided as follows on the details pane. They are denoted by a unique icon:

- indicates the number of transitions. Transitions include submit, updates, and other transitions.

- indicates the number of notes added to the item using the item actions or on item update.

- indicates the number of attachments added to the item. Attachments include adding files, URLs, and item links.

Expert Panel

You can select to display a list of suggested experts by clicking the Suggest 3 Experts link on the **Social Widget**. The suggested experts are a list of users who are ranked based on the number and kind of similar items that they worked on. The top three users from this ranked list are displayed.

Click on a suggested expert to display their contact information. If the user has a configured email address, you can choose to send the user an email by clicking on the email link.

The experts are found and ranked based on the following criteria:

- The title words in the item are used to search for similar items within the same project and subprojects. Similar items are found and ranked based on a weighted keyword search of the title and description within the items.

- Only items that have been in the same state in the past six months are evaluated.

- Deleted users are not included in the suggested expert list.

- The current user is not included in the suggested expert list.

Urgency, Impact, and Priority

An item's *Priority* determines the sequence in which items will be addressed. High priority items should be addressed quickly and escalated up the organizational hierarchy, if necessary. Lower priority items can be addressed in a less urgent manner, and they should not be re-prioritized to expedite their resolution.

The default Service Manager includes five levels of priority, with 1 being the highest priority and 5 being the lowest priority.

ITIL defines *Priority* as being based on the *Impact* to the business and the *Urgency* within which the resolution is required by the user or business. In other words, *Impact* is a measure of how business critical the incident is and *Urgency* is the speed required to resolve the incident. Service Manager automatically determines Priority after you have selected the Impact and Urgency for an item.

> **Tip:** Since there are additional elements that could be included in determining the priority, like scope, complexity, who is requesting the change, and resources required for resolution, submitters can override the automatically determined priority by selecting a new one in the **Priority** drop-down list.

> **Note:** Overall impact can be difficult to determine, and it is common to simplify impact by relating it directly to how many users are affected by the item. Serena Service Manager uses this approach and allows for three impact choices: **Enterprise**, **Department**, and **Single User**.

The following table explains how the priority is determined based on your selection for *Impact* and *Urgency*:

Table 1. Urgency, Impact, and Priority

		Impact		
		Enterprise	**Department**	**Single User**
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

Implementation Method

The automatic calculation is performed by JavaScript included on the **Submit** form.

You can make modifications to this process, for example by adding a new level of Impact, by performing the following changes in SBM Composer. Note that this change must be performed for each process app, such as Incident Management, Problem Management, and Change Management.

To update the JavaScript:

1. Open a process management app in SBM Composer, such as Incident Management.

2. Add the selection values to the Impact, Urgency, or Priority fields to the primary table. For example, for Incident Management, you would add the values to the **Incidents** table under Data Design.

3. Change the calculation of Priority by modifying the **calcPriority** script found on the Submit form. For example, suppose you added a new Impact value called CEO, in case the incident impacts the CEO directly, you could change the following line to include checking for the CEO value when setting the priority:

```
if ((impact == "Enterprise" && urgency == "High") || (impact == "CEO"))  \{
    SetFieldValue("PRIORITY", 1);
\}
```

Chapter 3: Serena Request Center

Serena Request Center is a user-friendly IT Service Portal, designed for the non-IT user. Request Center both advertises IT functions and allows users to access these operations in a visually appealing way. The simplified interface allows users access to the service catalog, their submitted requests, and the Knowledge Center.

Serena Request Center is ready for immediate use with its Starter Pack Services, custom forms, and request fulfillment workflows. The Starter Pack Services are created when you promote the Starter Pack Forms and Service Desk Process App included with SRC. The Starter Pack Forms are a collection of external forms that are used with the request fulfillment workflows in the Service Desk Process App. The forms are tailored for the service, which allows each form to be different, although they are based on the same request fulfillment workflow. The Service Desk Process App contains all of the request fulfillment workflows as well as Incident Management.

Users access the Request Center portal through the following URL:

```
http://serverName/tmtrack/tmtrack.dll?shell=srp
```

The following topics describe the functionality available in Request Center:

Key Benefits

- User-friendly, visually appealing interface into IT Service Operations.

- Pre-populated services.

- Custom submit forms tailored for request fulfillment.

- Instant access to important IT service announcements.

- Easy access to search articles in Knowledge Center.

- Users see a list of the items that they have submitted.

Starter Pack Services

After you have imported and promoted both Starter Pack Forms and Service Desk Process App, the Request Center is populated with the Starter Pack Services. These services make use of the request fulfillment workflows and the external forms found in Starter Pack Forms.

The following table shows a list of Starter Pack Services including the form used in Starter Pack Forms, the request fulfillment workflow used for each form, a description of how the workflow and request is meant to be used, and any required auxiliary tables.

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Building Security	New Access Badge	Atomic	New Access Badge requests are designed for new tracking requests for security badges for employees or other users. The New Access Badge submit form collects all of the pertinent information about the employee, including: • Requester details including requester name, project information and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request information such as name, department, manager, and access needs • Emergency contact information	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Install Server	New Server Install	Service Request	New Server Install requests are designed for new tracking requests for new server installations. The New Server Install submit form collects all of the pertinent information for a new server installation, including: • Requester details including requester, project information and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Department*, and *3*. • Hardware and Operating System. Note that the **Requested Operating System** points to the **Operating Systems** auxiliary table, which must be populated before submitting new items. • Permissions • Network configuration such as load balancing requirements and DMZ need • Backup configurations such as frequency of backups and retention periods • General Instructions such as if it requires monitoring and any attachments.	Operating Systems
Firewall Request	Firewall	Atomic	Firewall requests are for users who need to access a particular server that is outside the network firewall. The request gathers the basic details including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as source information and destination information. Source information gathers details about the source machine such as name, type, and IP address. Destination information is for the machine that is to be accessed. • Attachments.	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
New Hire Request	New Hire Request	Composite	New Hire requests manages the hiring of a new employee. The submit form is a wizard that walks you through multiple tabs, including: • Requester details including requester, project information and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Department*, and *3*. • General information about the employee, such as employee name, start date, job title, department, and office location such as cube number or remote location. • Computer tab collects information about the required computer and software needs. • Voice and data tab collects the information about phone and voicemail requirements. • Network tab collects information about VPN access and email setup. • Special Instructions include other set up requirements such as access to a printer, mainframe, or CRM tools. After the request gathers the information required for a new hire, it travels through the New Hire Request composite workflow, where the Level 1 Technician can then create subtasks from the item to manage the different tasks required, such as getting an access badge and new a PC request.	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Install Client Software	Client Software Installation	Requisition	Install Client Software request is designed for new tracking new software installations. The request requires financial approval before being sent to the purchasing. The request filters available software choices based on the department. The request collects all of the pertinent information for a software installation, including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as department, current operating system, requested software, and PC IP address. Note that the **Current Operating System** and **Client Software Requested** fields point to auxiliary tables, which must be populated before submitting new items. • Attachments	Client Software, Operating Systems

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Install New Desktop	New PC	Requisition	Install New Desktop are requests for new personal computers. The request gathers the requested computer type, along with the desired model and operating system. The request collects other pertinent information including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details include department, requested PC type and model, requested operating system, monitor requirements, speaker requirements, and fields for additional information. Note that the **Request PC Type**, **Requested PC Model**, and **Requested Operating System** fields point to the **Operating Systems** auxiliary table, which must be populated before submitting new items. **Note:** The available selections for Request PC Model and Request Operating System depend on the selection for Requested PC Model. The available selections are configured in the **Computer Types** auxiliary table. • Attachments	Computer Models, Computer Types, Operating Systems

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Install OS	Request to Upgrade OS	Requisition	Requests to Install OS are for users who need an updated operating system. The Requests to Install OS submit form collects the pertinent information for a new operating system, including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as Upgrade Reason, current and requested operating systems, and additional information such as drivers, adapters, and components. Note that the **Current Operating System** and **Requested Operating System** fields point to the **Operating Systems** auxiliary table, which must be populated before submitting new items. • Attachments	Operating Systems
Access to Network Printer	Network Printer Access	Atomic	Printer access requests are for users who need access to a particular network printer or need a printer to be added to the network. The request gathers the basic details including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as printer name, IP address, and any special features. • Attachments and work notes.	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
MSDN License Request	MSDN Account	Requisition	MSDN License Requests are for user accounts to access to MSDN. The request gathers the basic details including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as MSDN Account Level. • Attachments and work notes.	
Request New Desk Phone Voice Mail	Desk Phone Voice Mail	Atomic	Desk phone and voice mail requests track the setup of a new phone for an employee. The request gathers the basic details including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as recipient location and address. • Attachments and work notes	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Mobile Device Request	Mobile Device	Requisition	Mobile device requests are designed for employees requiring a new mobile phone or pager. The requests collect the pertinent information about the device, including: • Requester details including requester, project information, and cost center. The **Urgency**, **Impact**, and **Priority** are automatically set to *Medium*, *Single User*, and *4*. • Request details such as Mobile Carrier, Mobile Device, and options. Note that the **Mobile Device** selections are based on the **Mobile Carrier** selection. These two fields are populated based on their respective auxiliary tables. You must add data to the tables before you can submit a new item. • Attachments	Mobile Carrier, Mobile Device
Backup Request Facilities Issue Facilities Suggestion Network Port New Mailbox Office Move Request Password Reset Printer Service Request	SR - Submit (found in Service Desk Process App)	Service Request	These services were included in previous releases of Request Center. They are included here as well, using the same default Service Requests workflow; however, each of the services now has an individual project created for it.	

Service	Form	Request Fulfillment Workflow	Description	Auxiliary Table
Report an Issue	IM - Submit (found in Service Desk Process App)	Incident Management	This service is for submitting incidents into Incident Management. Refer to Chapter 5: Incident Management [page 49] for more information on Incident Management.	

Request Center Overview

Request Center is a portal into the IT Services, where end users can access the important and pertinent information quickly. The Request Center is for tailored for end users that require limited access to Service Manager and who do not need to be burdened by the additional functionality found in the User Workspace.
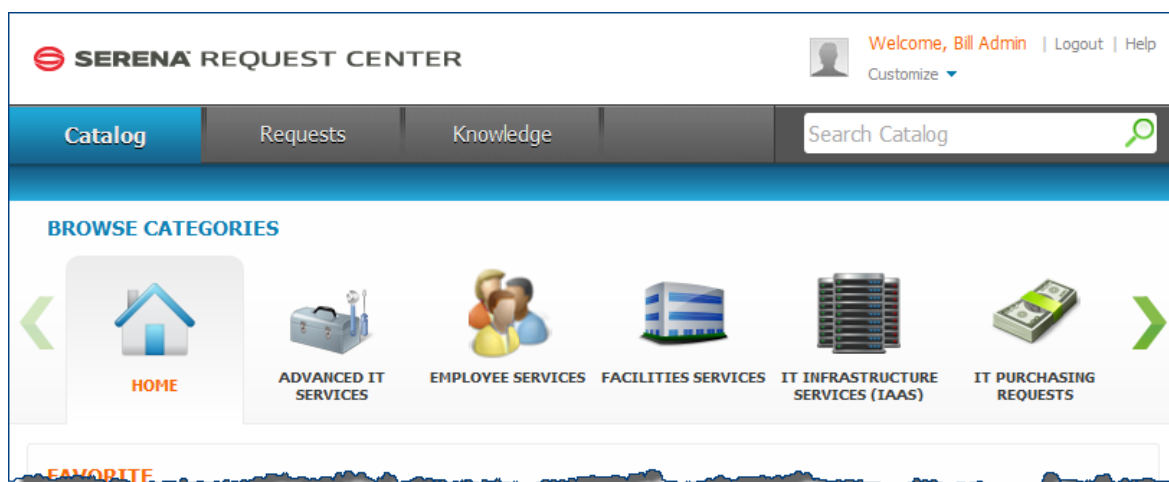
End users access Request Center through the following URL:

```
http://serverName/tmtrack/tmtrack.dll?shell=srp
```

Request Center consists of the following views:

- **Catalog** tab where users can submit requests into applications or access external URLs as determined by the IT Administrator.

- **Requests** tab where users can monitor the items that they have submitted, alerting them if any item requires action such as adding information.

- **Knowledge** tab where users access Knowledge Center articles.

Urgent announcements that were submitted into Knowledge Center are displayed in the announcement bar, which appears below the banner.

Users can click the **Help** button to display inline help for understanding how to use the portal.

Both the banner and the Contact Info are configurable by the IT Administrator. The IT Administrator can choose the logo and title to display in the banner. The IT Administrator can also choose which information to display in the Contact Info dialog. See Configuring Request Center [page 33] for more info.

Service Catalog

The service catalog view appears on the **Catalog** tab in Request Center. The service catalog is a collection of IT services defined by an IT administrator.

The end users choose from the available services by clicking on the appropriate icon. The services are organized by category, allowing the end users to filter the services based on categories. Users navigate between the categories by browsing the categories in the ribbon bar. Selecting a category will display only service actions assigned to that category.

Users access a service by clicking on the title. The user can display detailed information on a particular service by clicking the summary to show the details. Users can search for services by entering a keyword to search for in the search field. The search supports has limited wildcard support, such as *.

Certain services appear on the Home page for all users, and they are divided into **Favorite**, **Featured** and **What's New** services.

The IT Administrator defines what services appear in each section when customizing Request Center. For information on configuration, see Configuring Request Center [page 33].

Requests View

The Requests view displays items that the user submitted. By default, the items are grouped by request date. A symbol represents the status of each item:

- signifies active items that are currently waiting for action by other users.

- signifies items that the user must act on. These items may require that the user adds information or approve the item. Click on the item to display the form where you can update the item.

- signifies that the items are inactive.

The following actions can be performed on the **Requests** tab:

- Filtering items by selecting **Active**, **Follow Up**, or **Inactive**

- Sort items by selecting **Request Date**, **Last Update**, **Type**, **Owner**, or **State**

- Searching for items using the search field

- Displaying the details of an item by clicking on its title

- Displaying the Workflow History of an item by clicking the magnifying glass adjacent to the title.
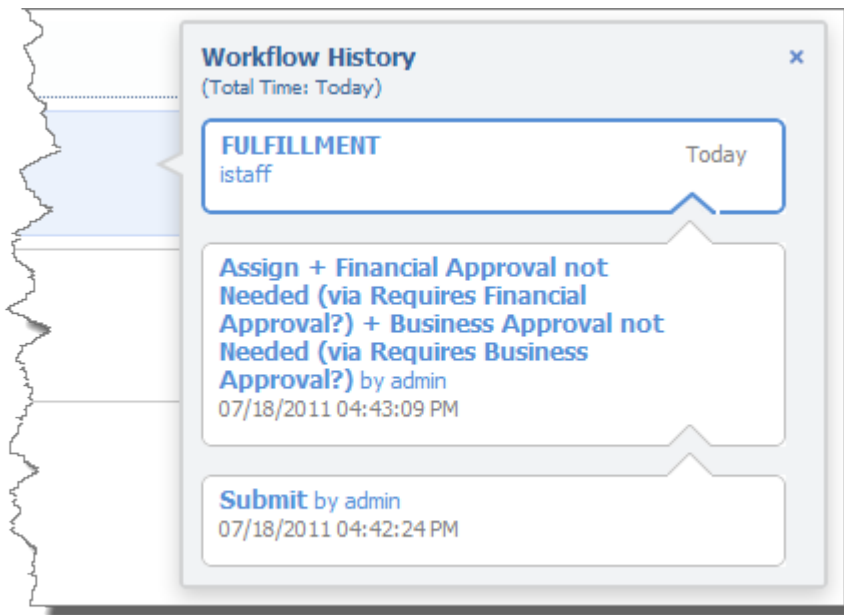
The Requests view depends on the **Request Center - My Request** report that is included with the Incident Management application. The report is a multi-table report that displays all of the items that the user has submitted into Incident Management, Service Desk, and Knowledge Management.

> **Tip:**
>
> By default, the **Request Center - My Request** report only contains items that have been modified in the past 30 days, meaning that items that have not been modified for more than a month will not appear on the report. This setting eliminates the clutter of older items from the Requests view.
>
> The report is also limited only to items in Service Desk Process App. You may want users to see requests from other tables as well. For example, if you have Service Manager installed, you may want to modify this report to span the Incident Management, Problem Management, Change Management, and Knowledge Management applications.
>
> Administrators can modify the default report to change the filters or the included tables. The report is in the Incident Management application and is titled **Request Center - My Request**. The updated report must be saved with the same reference name of **SSMMyRequests**.

Knowledge Center

Knowledge Center is the online interface into the Knowledge Management system available with Service Manager. Users access Knowledge Center by logging into Request Center and selecting the **Knowledge** tab.

Knowledge Center lets you perform the following actions:

- Search for articles within Knowledge Center by entering keywords in the search field on the **Knowledge** tab.

- Sort the search results by latest added, top rating, most popular, or most commented. **Best** is based on cumulative ratings and **Popular** is the total number of views.

- Filter results based on category by selecting the category in the list.

- Group results by article category or type.

- Display detailed view by clicking on the article's title.

- Add comments and rate the article in the detail view by clicking **Add your own comment**. Choose the number of stars to give the article and enter any comments.

  > **Note:** You are only allowed one comment and rating per article. Subsequent comments will replace the original comment.

- View important IT announcements, such as possible outages. Similar to the other tabs, the announcements appear below the banner.
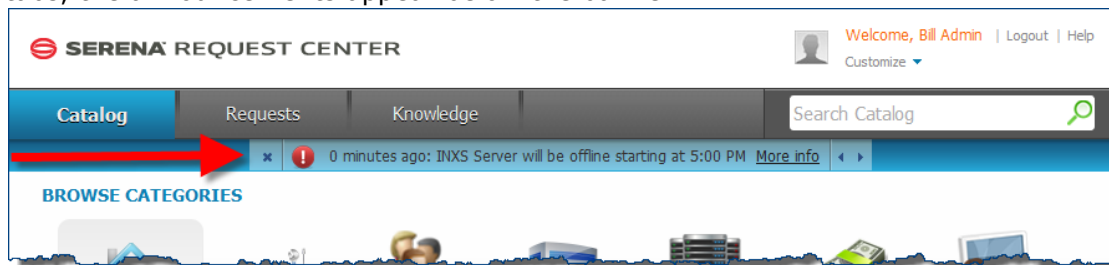
> **Note:** If you have publish privileges, you will also be allowed to view expired articles and update articles. Select **Include Expired** to include expired articles in your search results. In the detail view, click **Update This Article** to begin the update process for the article.

Both the Knowledge Center articles and announcements are managed with Knowledge Management. For more information, see Chapter 10: Knowledge Management [page 105].

Configuring Request Center

> **Important:** Before allowing users access to Request Center, promote all of the snapshots to your environment. This allows the data for Starter Pack Services to be available when you log in.

If you have remote administration privileges, you are able to customize Request Center. All customizations that you make to Request Center will affect all users.

- Adding Categories [page 34]

- Defining Services [page 35]

- Changing Logo, Announcements, and Contact Information [page 38]

- Troubleshooting [page 39]

- About the Image Picker [page 39]

> **Note:**
> When you log into Request Center as an administrator, you will see the following differences:
>
> - In edit mode, invalid services will be marked with alert icons ⚠. Invalid services may point to a deleted project or to a project that is used by another service.
>
> - In view mode, invalid or hidden services appear. This allows administrators to modify invalid services instead of having to create a new one. Invalid and hidden services are not seen by end users.

The following topics explain how to customize Request Center.

Adding Categories

Categories group service actions for easy navigation.

To add a new category:

1. Log in to Request Center (`http://serverName/tmtrack/tmtrack.dll?shell=srp`) with a user account that has administrator privileges.

   > **Restriction:** For on-premise installations, the administrator needs either a **Regular User** license and **Remote Administration** privilege or a **Managed Administrator** license and **Global Administration** privilege. For on-demand installations, the administrator needs to be part of the **Administrator** group.

2. Select **Customize | Service Catalog**.

3. Click **+ Category** button.

4. Choose an image for the service by clicking **Change image**. You can choose from existing images or insert a URL. For best results, use an image that is 64 x 64 pixels. For information on the image picker, see About the Image Picker [page 39].

5. Enter a **Name** and **Description** for the category.

6. Select the **Display Order** for the category by dragging the slider. The lower the number, it will appear further to the left in the display.

7. Click **Save** to save the new category.

The new category will appear in the selection list. The categories are organized as follows:

1. Home category is always first.

2. Other categories are arranged by display order and then alphabetically if the display order is the same.

To edit, clone, or delete a category:

1. Select **Customize | Service Catalog**.

2. Select the category to edit, clone, or delete.

3. Click on the appropriate icon to edit, copy, or delete the category.
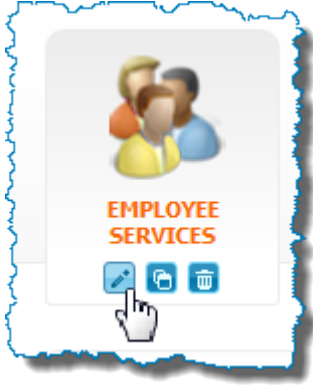
Defining Services

IT service actions are available to end users through Request Center. Service actions allow you either to submit a new item into a Service Manager process or to access a URL. Service actions are laid out in a user-friendly format within Request Center. Users can browse services by their category or by searching for them with the search filter.

To add a new service action:

1. Log in to Request Center (`http://`*serverName*`/tmtrack/tmtrack.dll?shell=srp`) with a user account with administrator privileges.

2. Select **Customize | Service Catalog**.

3. Click **+ Service** to add a new service operation.

4. Choose an image for the service by clicking **Change image**. You can choose from existing images or insert a URL. For best results, use an image that is 32 x 32 pixels. For information on the image picker, see About the Image Picker [page 39].

5. Enter a **Name** and **Summary** for the new service operation. The summary appears as a quick description in Request Center.

6. Change the **Category** by choosing the category from the drop-down menu.

> **Tip:** Selecting a category before clicking add service will pre-populate the category field with the selected category.

7. Enter a longer description in the **Description** box. The long description appears when the end user expands the service action in Request Center.

8. Enter the **Charge Back** cost. The Charge Back cost is the cost that end user or the end user's department will incur due to the successful completion of the service action. Note that this field is only displayed to the end user in Request Center when values are entered.

9. Choose to display the service operation under the **Favorite**, **What's New**, and **Featured** sections under the home view of the Catalog tab by checking all that apply.

10. Select the **Display Order** for the service by dragging the slider. The lower the number, the higher it will be in the display order.

11. Under **Visibility**, select **Show in Catalog** to display the service to the end user. Hidden services will not appear to end users but they will still appear to administrators.

12. Select the option either to submit into an SBM process app or to show an external URL.

    • For an SBM process app, you must define what project to submit into and which submit form to use. You can specify the **Type** and pre-populate the **Title** field for the new item as well. The following table explains the different fields available on this form.

Fields	Description
Process App	Choose the process app which contains the project to submit into.
Project	Select the project to submit into. There is a one-to-one relationship between projects and services. Projects used by another service are marked and cannot be selected.
	You can modify and create projects directly. Select **Open Project** to open the selected project in SBM Application Administrator. Select **Add Project** to open SBM Application Administrator to the top level view, where you can click on **Projects**, navigate to the desired parent project and add a new sub-project. After adding the project, click 🔁 to refresh the project list.
Submit Form	Select a submit form to use for submitting the item. This form will override the submit form defined in the project. The form can either be in the process app with the primary table or in a process app that has forms which reference the primary table, such as the forms contained in the Starter Pack Forms process app.
	Note: Service Desk Process App includes additional forms which are designed for transitions other than submit. Do not choose these forms, since the JavaScript included on the forms may cause unexpected behavior like a disappearing form.
Type	Select an item type for the issue to be submitted. The item types are based on the project that you selected.
Title	Enter text which will be pre-populated in the title field of the item.

Fields	Description
SLA Summary	The SLA Summary can either be a text entry or a list of SLAs for the selected project.
	The text field can be modified and it will appear to the end user when they view the details of the service. If the project has SLAs defined, instead of the text box, you will see a list of defined SLAs and their descriptions.

Note:

- There is a one-to-one relationship between projects and services. Alert icons 🔴 will appear in the portal if multiple services share the same project.

- If the user does not have permissions to submit into the application or project, the service will not appear in Request Center for that user.

Important: Choose a project that allows submissions. If the project does not allow submissions, then the user will receive an error when selecting the service. The following is a sample error:

```
An error occurred while processing the last request.
....
Project doesn't allow submitted items:
```

- For an **external web page**, enter the URL in the field. Choose whether to display the link within the Request Center or in a new window.

  You can also enter an **SLA Summary**, which is a description of the service level that the end user should expect. The SLA Summary field is displayed to the end user in Request Center when values are entered.

To edit, clone, or delete a service action:

1. Select **Customize | Service Catalog**.

2. Select the service action to edit, clone, or delete.

3. Click on the appropriate icon.
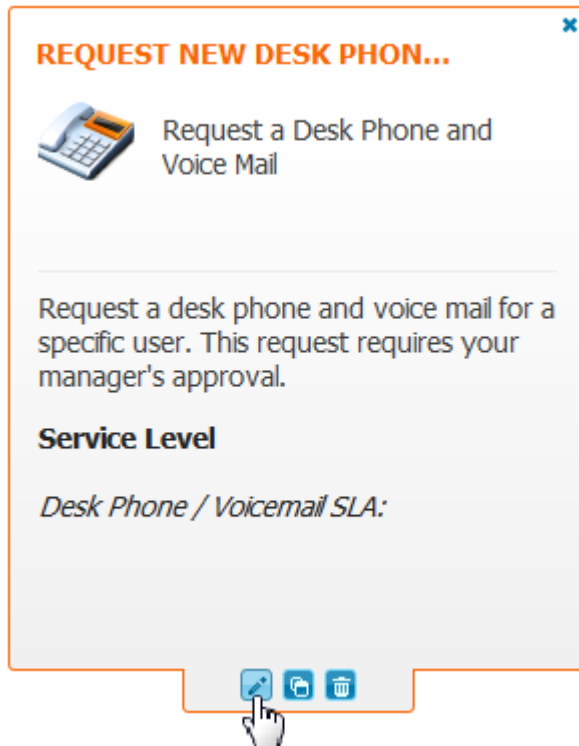
Changing Logo, Announcements, and Contact Information

The look and feel to Request Center is easily customizable, allowing you to tailor the portal. Possible changes that you can make include:

- Changing the graphic that is displayed in the title bar.

- Modifying the information and hyperlink that appears alongside the graphic.

- Turning on or off the announcements that are added to Knowledge Center.

- Changing the contact information that appears in the **Contact Info** link .

> **Important:** Remember that Request Center customizations affect all users.

To customize the display properties of Request Center:

1. Log in to Request Center (`http://serverName/tmtrack/tmtrack.dll?shell=srp`) with a user account with administrator privileges.

   > **Tip:** If you were already logged in to the Request Center, refresh your browser. This ensures that you have the latest updates to Request Center and that you will not overwrite someone else's updates. When you log in, the Request Center properties are cached locally. Failing to refresh will use the cached properties instead of the latest properties in the database.

2. Select **Customize | Request Center**.

3. Change any of the following:

Customization	Notes
Title	The title appears alongside the logo. You can apply formatting to the text using the formatting toolbar.
Image (URL)	Enter a URL to your corporate logo. Remember this URL must be accessible by all users from Service Manager. For example, do not enter a logo that is located in a restricted domain that is not accessible by all users.
Image Link	Enter a URL which a user a will be directed to if they click on the logo.
News/ Announcements	Select **Show in Request Center** to display urgent announcements to users in the announcement bar, underneath the banner. You can set the **Refresh Interval** for the urgent announcements by selecting the minutes for a refresh. For more information on creating and publishing urgent announcements, see Chapter 10: Knowledge Management [page 105] .
Contact Info	Add a title and content for the contact info link. The title affects both the dialog title and the link name. HTML is not supported in the title field. The contents appear in the dialog. Use the formatting toolbar to apply styles and formatting to the content. You can hide the Contact Info link by deselecting **Show in Request Center**.

4. Click **Save**.

Troubleshooting

If the SBM User Workspace is displayed instead of the Request Center when you access the URL, verify that:

- Request Center has been installed by running the Service Manager installer.

- IIS Web Server has been restarted after installing Service Manager.

About the Image Picker

The image picker is used to pick images for categories and services in Request Center, as well as for picking images when creating Knowledge Management categories.

The image picker comes with a collection of images that are arranged into multiple groups. You can choose to view all images or select a group to view only images in that group.

Choose the image by selecting the image and clicking **OK**.

> **Tip:** Instead of picking the image, you can insert a URL to an image in the text field. Remember that the image location must be accessible by all Request Center users.
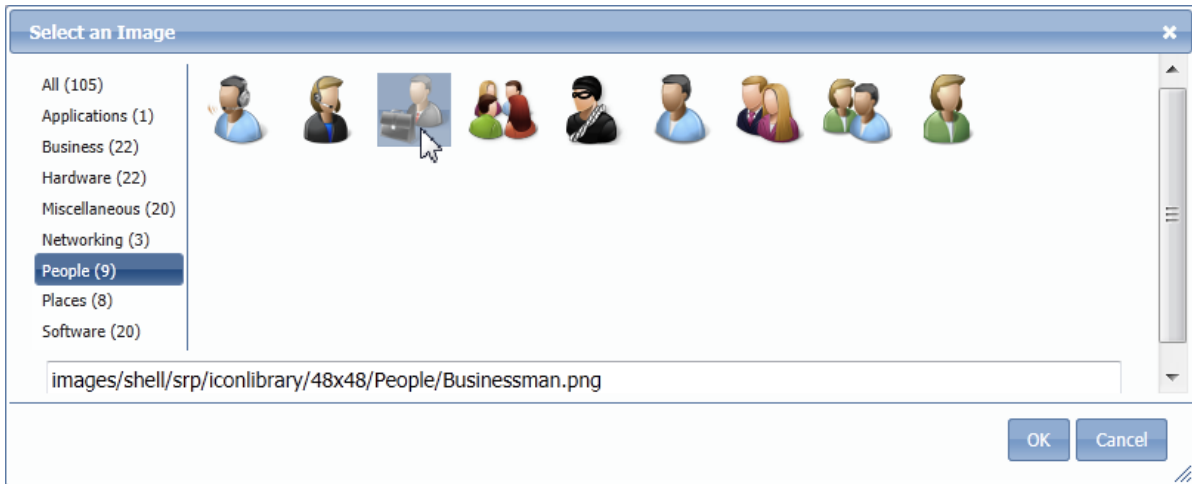
Adding New Images to Image Picker

On-premise installations can add new images to the image picker. The administrator must perform the following steps on the SBM Server:

1. Add the new PNG image files to the `32x32`, `48x48`, and `64x64` folders in the following directory:

   SBMinstallationDirectory`\Serena\SBM\Application Engine\bin\images\shell\SRP\iconlibrary`

   > **Note:**
   >
   > - The image size should be 32 by 32 pixels in the `32x32` directory. The images in this directory are used for the image picker.
   >
   > - The image size should be 48 by 48 pixels in the `48x48` directory. The images in this directory are used for the services.
   >
   > - The 64 by 64 images are placed in the `64x64` directory are used by both Request Center categories and **KM Categories**.

2. Update **serviceimages.js** and **catalogimages.js** to include the new images. These files are found in the following directory:

   SBMinstallationDirectory`\Serena\SBM\Application Engine\bin\javascript\shell\SRP`

3. Open SBM System Administrator and go to **File | Put Files Into Database**. This will prevent the new image from being deleted the next time IIS is restarted.

About the Service Desk Process App

The Service Desk Process App contains both the Incident Management and the Service Request fulfillment workflows. This app is included with both Serena Service Manager and Serena Request Center. The Service Desk Process App is referenced by Starter Pack Forms and the pre-populated service definitions found in Serena Request Center.

Note: There are two Service Desk Process Apps, one found in Serena Service Manager and Serena Request Center. They are identical.

For detailed information on the workflows found within the Service Desk Process App, refer to the following:

- Chapter 5: Incident Management [page 49].

- About Starter Pack Forms [page 41]

About Starter Pack Forms

The Starter Pack Forms process app contains a collection of forms that are used in Serena Request Center for submitting and viewing items. The Starter Pack Forms are external forms that reference the Service Desk Process App. The forms are designed for use with the different service request fulfillment workflows available in the Service Desk Process App.

Each of the Starter Pack Forms has two versions, one for the submit transition (Request) and one for the state forms (State). When installing and deploying the apps in Serena Request Center, unique services and projects are created for each pair of these forms.

Tip: The services and projects are listed in the table under Starter Pack Services [page 21] .

The request form is used to submit items into the projects. The form is made up of both fields referenced from the Service Desk Process App and from multiple edit box controls that gather information. The edit box controls allow the gathering of information without having to clutter the Incident Management primary table with fields. After the submit is completed, the data from the edit box controls as well as the fields are written into the **Description** field of the item. This allows you to see the data entered in all of the fields.

The Starter Pack Forms state forms are displayed on the **Request Data** tab for submitted items. The tab contains many of the custom fields for that item. The state form that is displayed is determined by the value of the **RequestForm**, which is set when the original item is submitted. This allows the state form that is paired with the original submit form to be displayed.

Note: The Starter Pack Forms significantly improve the ease at which forms can be updated and customized in the request fulfillment workflows. Instead of having to modify the main process app for every change to forms, modifications are made in the Starter Pack Forms process app. The workflow does not have to be modified since the custom submit forms are determined when setting up the services in Request Center. The display of the accompanying custom state form on the **Request Data** tab requires only two state forms on the main workflow, while allowing the display of custom fields appropriate for the submitted item.

In addition to the specialized forms, there are three generic forms which you can use as a basis for creating other specialized forms. To use as this form as template, right-click on the form and choose **Duplicate**.

The following table describes these three forms.

Form	Description
Submit Template	This default template can be used as a basis for creating a simple submit form. The form includes the basic fields such as requester, urgency, impact, and priority, as well as other details such as required date and cost center. The **Request Details** tab contains space to add additional fields. The Hidden Fields is a place for you to place your hidden fields.
Submit Template (Wizard)	The Wizard template can be used as a basis to create a multi-page submit form. This form is useful for collecting more data on the submit process. When a user clicks **Next**, the next tab in the submit form is displayed. This allows the user to progress through each tab, adding the required information, while maintaining a clutter free page.
State Template	The State template is a simple state from that contains the basic fields laid out to match the submit forms. You can include this state form as an embedded form on the tab of your item.

Chapter 4: Service Level Agreements

Service Level Agreements (SLAs) define the level of service that an organization commits to its customers. Individuals have different reasons to monitor SLAs. For example, as a technician, you need to know about SLAs that apply to your items so you can prioritize your work and understand if you are at risk of violating any of them. As a manager, you need historical information to measure how well your organization conformed to SLAs and forecast information to ensure that active items are not in danger of violating them.

In the SBM User Workspace, you have visibility into SLAs in the following ways:

- You can customize and view SLA reports that include past performance and current risk information in various formats. (SLA reports only show data if projects have SLAs defined for them, and if one or more services have been associated with those projects in Serena Request Center.)

- If the SLA widget control is included on state forms, you can view the status of SLAs that the current item is either in violation of or at risk of violating.

- You can subscribe to SLA notifications

The following list contains examples of SLAs that can be tracked using the SLA feature:

- High-priority items should be assigned to a technician within one business hour.

- High-priority items submitted by "Platinum" customers should be assigned to a technician within 30 minutes.

- High-priority items should be resolved within three business days.

- 99% of hardware requests should be completed within three business days of approval.

- No item can be in a "New" state for more than 3 business days.

About the SLA Widget

SLAs are used to review and monitor how your organization responds to service requests in comparison to customer commitments. SLA rules and metrics are defined by your administrator.

The SLA widget, which can be included on state forms, contains the status of the current item for each SLA that applies to it. Initially, the most severe status is displayed. The complete status list can be seen by clicking the arrow on the widget.

The list can contain the following values:

- **VIOLATED**, **HIGH**, **MEDIUM**, or **LOW** means the item is in violation of this SLA or at risk of violating it. The risk level is estimated in terms of time remaining to comply with the SLA. For example, an item is in violation if 0% of the allotted time remains, at high risk if 25% of the time remains, at medium risk if 50% of the time remains, and at low risk if 100% of the time remains. An item always starts the SLA process at low risk.

If **(Pending)** is appended to the value, the item is in a paused state, in which time is not counted against the SLA.

- **COMPLETED** means that the item has reached the "end state" defined in the SLA. If **(VIOLATED)** is appended to this value, the item was in violation when it reached this state.

- **No SLA Status** means that no SLA currently applies to the item.

When the status is hovered over, additional information is displayed. This information includes:

- **Name**

- **Description** (if provided)

- **Type**: **SLA** or **OLA** (Operational Level Agreement)

  > **Note:** SLAs and OLAs are defined and processed in the same way. OLAs typically monitor internal commitments that ensure that SLAs are met.

- **Date**: The date that the item violated the SLA or is expected to move to the next risk level. In the case of the **COMPLETED (VIOLATED)** status, the completion date is displayed, not the date the item violated the SLA.

  > **Important:** An SLA includes one or more "clauses," or rules. In addition to duration and severity percentages, the clause can define the portion of the workflow to which it applies.
  >
  > For example, a clause could apply to the range of states from the "New" to "Assigned" states, inclusive. Another clause in the same SLA could apply to the range of states from the "Assigned" to "Completed" states, inclusive. This means that if an SLA with multiple clauses applies to an item, the widget could show multiple status values, some of which may not be current.
  >
  > Using the previous example, the list would include **VIOLATED** if the item was not assigned to a technician within the allotted time. However, after it was assigned, if only 50% of the time for the technician to complete the item has elapsed, the list would also include **MEDIUM**.

About SLA Reports

SLA reports allow you to review and monitor how you and your organization respond to service requests in comparison to customer commitments. SLA rules and metrics are defined by your administrator.

To run an SLA report, click the **Reports** link, and then click **Access SLA Reports** under **Advanced Tasks**. The SLA report page contains two tabs: **Past Performance** and **Current Risk**.

The report page also contains a report filter that lets you change the criteria for the reports. You can either apply the criteria to the current report or save the criteria to be used in the next report.

Report Filter

To open the report filter, click the **Define Filter** link on the report page.

- To specify which services to include in the report:

  1. Click **Select Services**.

  2. In the dialog box that opens, select a service. Move it to the right to select it or to the left to remove it. To move it, click the plus or minus icon or double-click it. You can also drag a service to the right to select it. To add or remove all services, click **Add all** or **Remove all**.

  3. Click **Select** to close the dialog box.

- *Past Performance reports only:* To change the date range, click in the date box. From the menu that opens, select a specific date range or click **Date Range** and then select a start date and end date from the calendars. Alternatively, you can type over the date in the **Date Range** box, or click the **Prev** or **Next** arrows to bring the date range backward or forward by six months.

- *Past Performance reports only:* To change the threshold, type over the number in the **Performance Threshold** box. For example, **75** means that 75% or more of items meeting the SLAs is acceptable, and less than 75% is unacceptable. To raise the expectation, change the number to something higher.

- *Current Risk reports only:* Select the **Items I Own** check box if you only want to see data that is relevant to items for which you are the primary or secondary owner.

- Click **Apply** to apply the settings to the current SLA report and close the dialog box. Click **Save Settings** to save the settings to the database so they are applied to the next SLA report you run.

Past Performance Reports

Past Performance reports provide historical information. By default, data for all services from the last six months is displayed, with a performance threshold of 80%. This means that over the last six months, an overall SLA "passing" performance level of 80% or greater (with an overall "violation" performance percentage of less than 20%) is considered acceptable for normal operation. To change the report criteria, see "Report Filter," above.

The following Past Performance reports are available:

- **Aggregate Performance**—Measures the aggregate performance level of all services included in the report. This is the percentage of items that are within the acceptable range of the performance threshold, which is specified in the Report Filter (see above). The red part of the gauge represents the percentage that is under the performance threshold; the green part represents the percentage that meets or exceeds the performance threshold. The goal is for the needle to point in the green area.

- **Performance Breakdown**—Shows each service name, the SLAs associated with each service, the SLA threshold specified by an administrator during the definition of the SLA, and the actual SLA performance. The SLA performance value is displayed in red if it falls into the unacceptable range.

- **Violations by Service**—Shows the service names and the number of items for each service that are in violation of the SLAs defined for it. You can click a bar in the chart to drill down to the next chart.

- **Violations by SLA for Service: "*service name*"**—Shows the number of items that are in violation of each SLA defined for the service. By default, the report format is a chart; click the **Listing report** button to change the format to a listing report. You can click a bar in the chart to drill down to the next report.

- **Violations for SLA: "*SLA name*"**—Lists each item that is in violation of the SLA. For details about the content of the report, see "Listing Reports," below. Click the link in the **Item Id** column to open the item. To close the item and return to the report, click the **X** at the top right corner of the item.

Current Risk Reports

Current Risk reports are calculated using the time and risk values defined for each SLA. By default, data for all services is displayed in the reports. You can select specific services to monitor and specify that only data for items you own is displayed. To change the report criteria, see "Report Filter," above.

The following Current Risk reports are available:

- **Risk Projection**—Shows the number of items from all services included in the report that are in violation of or are at risk of violating the SLAs associated with them. Violations and risk categories are stacked horizontally in the bar in different colors; click one to view the corresponding chart on the right.

- **Violation/*Risk Category* Items by Service**—Shows the service names and the number of items for each service that are in violation of or at risk of being in violation of the SLAs defined for it. The name of the chart changes depending on what is clicked in the Risk Projection report. You can click a bar in the chart to drill down to the next chart.

- **Violation/*Risk Category* Items by SLA for Service: "*service name*"**—Shows the number of items that are in violation of or at risk of being in violation of each SLA defined for the service. By default, the report format is a chart; click the **Listing report** button to change the format to a listing report. You can click a bar in the chart to drill down to the next chart.

- **Violation/*Risk Category* Items for SLA: "*SLA name*"**—Lists each item that is in violation of or at risk of being in violation of the SLA. For details about the content of the report, see "Listing Reports," below. Click the link in the **Item Id** column to open the item. To close the item and return to the report, click the **X** at the top right corner of the item.

Listing Reports

Some of the SLA reports are in a listing report format. Most, but not all columns are displayed by default. To display hidden columns, and to optimize the reports for your screen, right-click in any column header and select or clear check boxes for columns you want to see or hide. In these reports, you can also click a column header to sort rows in ascending or descending order. Descriptions for some of the columns follow:

- **Estimated Date:** The date the item will violate the SLA if the item does not complete the SLA process within the "duration" that was defined for the SLA. This date should move forward to account for the time the item spends in "paused" states.

  > **Note: Waiting for Input** is an example of a paused state in which a technician waits for a customer to provide information needed to proceed with the item.

- **Completion Date:** The date the item left the "end state" that was defined for the SLA.

- **Elapsed Time:** The amount of time since the item entered the "start state" that was defined for the SLA, with the exception of the amount of time it spent in "paused" states.

- **SLA Type:** SLA (Service Level Agreement) or OLA (Operational Level Agreement). SLAs and OLAs are defined and processed the same way. They differ in that SLAs typically address customer commitments, while OLAs typically address internal commitments that ensure that SLAs are met.

- **SLA Clause:** The name of the clause that applies to the item. Clauses define the criteria under which items are monitored; for example, a "High Priority Incidents" clause defines SLA timing and conditions for high priority items, while a "Normal Priority Incidents" clause would define less stringent criteria.

  > **Note:** If an item was deleted or if you do not have privileges to view an item, it will not be included in the listing report. It will, however, be included in the chart reports.

Chapter 5: Incident Management

Incident Management focuses on restoring services to normal operation after service interruptions as quickly as possible and minimizing the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

The following topics explain the features of Incident Management in the Serena Service Manager.

- Incident Management Overview [page 49]

- Incident Management Workflow [page 56]

- Incident & Service Requests Dashboard [page 57]

- Satisfaction Dashboard [page 59]

- Incident Management Roles [page 60]

> **Note:** The Incident Management application is contained within the Service Desk Process App.

Key Benefits

- Incident prioritization and classification based on ITIL standards.

- Graphical indicators for easier process visualization.

- Incident workflow according to ITSM best practices.

- Ability to relate existing Known Errors to new incidents.

- Ability to track first call resolution rates.

- Reporting dashboard to monitor possible problem areas and resolution rate.

Incident Management Overview

The incident management workflow addresses the following areas:

1. Incident Creation [page 50]

2. Incident Classification and Initial Support [page 51]

3. Incident Investigation and Diagnosis [page 53]

4. Incident Resolution and Closure [page 54]

5. Incident Monitoring and Communication [page 55]

6. Incident Reporting [page 56]

1. Incident Creation

Incident creation is known as submitting incidents in Serena Service Manager. Two primary actors responsible for submitting incidents are end users and IT Service Desk staff.

Users can submit their incidents using the Request Center, SBM User Workspace or by e-mail.

> **Note:** Incidents can also be submitted automatically from another application using Web services. For example, if you have the Service Manager integration to Microsoft Operations Manager, incidents will be submitted automatically with Web services when certain issues arise.

To create a new incident using SBM User Workspace:

1. Select the **Service Desk** application tab.

2. Select **Submit** from the navigation pane on the left.

3. Click **Submit to My Preferred Projects** and choose an incident Management project to submit into from the project tree.

4. On the Submit form:

   - Choose the **Urgency** and **Impact** from the drop-down lists. **Priority** is calculated automatically described in Urgency, Impact, and Priority [page 17], but the value can be overridden.

   - Enter a **Title** and **Description**.

     > **Note:**
     >
     > A keyword search of Knowledge Center is performed after you have entered a **Title** and moved focus to another field. When articles exist in the Knowledge Center that match the title words, a message will appear informing you of the number of matches. Click **View** to look at matching articles.

     If one of the articles addresses your issue, open the article by clicking on the title and choose **Yes, cancel submit** to cancel the submit process.

   - Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.

5. Click **Submit** to create the new incident.

Submitting Incidents Using E-mail

You can configure SBM to accept new incidents through e-mail.

For on-premise installations, information on configuring SBM to handle e-mail submissions is available in the *SBM System Administrator Guide*.

For on-demand installations, contact Serena Support for configuring e-mail submissions.

Submitting Incidents from an Existing Incident

The incident management workflow has two methods for creating incidents from within the workflow. These are accessible under the **More Actions** menu.

- **Copy Incident** - Creates an identical copy of the existing incident.

- **Post New Incident** - Opens the submit form with the fields populated based on the existing incident. The values can be edited in the new incident before you submit the item.

2. Incident Classification and Initial Support

Incident classification includes setting priority, performing incident matching, and linking incidents to configuration items. Initial support includes finding an existing workaround or matching with other existing errors.

In the **Classification** state, the Service Desk staff review the issue and determines how the incident should be handled. The following actions may be available to you for updating and routing the incident. Your actual available actions depend on your role:

- **Assign** the incident, which automatically routes the item based on the answer to Major Incident.

  - **If item is not a major incident**, the issue is assigned to the Level 1 Technician for additional review.

    Note: The **Level 1 Technician** selection list includes users who are in the *Level 1 Tech*, *Level 2 Tech*, and *Level 3 Tech* roles. This allows a Level 2 Tech or Level 3 Tech to be assigned level 1 incidents if the tech is available.

  - **If item is a major incident**, the incident is immediately escalated to the *Incident Manager*.

    Note: Major incidents require the immediate attention of the incident manager. The incident manager may pull in the appropriate resources to quickly restore normal service operations. It may also require the incident manager to coordinate with problem management to find the root cause of the major incident to prevent its recurrence.

- **Resolve** the incident, noting whether it was resolved on the first call.

- **Update** with additional information from the end user.

The following options are available under the **More Actions** menu. They allow you to move the incident to another project, to merge the incident with other incidents, or to create duplicate incidents:

- **Delete** the incident, removing it from the system.

- **Recategorize** moves the incident to another project within Incident Management. Use this transition to change the Incident to a Service Request.

- **Merge Incident** ties together the current incident with an existing incident using Parent/Child relationships. See .

- **Copy Incident** creates a duplicate of the incident in the same state as the current incident. You cannot modify the values when the item is created.

- **Post New Incident** creates another incident based on the current incident. You can modify the values in the new incident on the Submit form and the new incident begins at the start of the workflow.

- **Remove Problem Link** lets you remove a problem link to the incident. The problem is not deleted, only the relationship between the incident and the problem.

In this state, users such as Service Desk staff can choose from the following:

- Attach a file to an incident on the **Notes/Attachments** tab.

- Choose an action such as Send an E-mail from the **More Actions** drop-down list.

When updating or transitioning the incident, you can modify data in the incident. The following describes the information to add in the fields, and how the information is used:

- The **Incident Type** is usually set automatically during submit; however, technicians may be allowed to override the value.

- Choose the **Urgency**, and **Impact** from the drop-down lists. **Priority** is calculated automatically as described in Urgency, Impact, and Priority [page 17], but the value can be overridden.

- Search for a **Configuration Item** to relate to the request. The configuration item categorizes the incident by automatically adding an incident category, incident sub-category, and incident sub-category type (if defined).

  Note: Selecting a configuration item is important as the CI is used to show related CIs and to show links to existing problems.

- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.

- After selecting the Configuration Item, you can view other active incidents for that item by displaying the **Active Incidents** tab.

Merging or Linking Incidents

Merging or linking incidents creates a parent/child relationship between the incidents that you are merging. The parent becomes the main item, which continues to move through the workflow as updates are performed. The children move to the **Linked to Parent** state, indicating that they are no longer the main item. When you view the item, users a see a note across the top that says "**This incident has been MERGED...**." The parent issue is then displayed on page underneath the message.

When the parent is resolved, the children are automatically resolved as well. The resolution notes from the parent are added to the children.

To merge incidents, select the **Merge Incident** action. On the **Merge Details** tab, choose whether the incident should become the child or parent:

- If you chose the incident to become the **Parent**:

  1. Select the incidents to add as children and click **OK**.

2. The children will be moved to the **Linked to Parent** state.

3. The parent continues to move along the workflow.

4. When the parent is resolved, all children are automatically moved to the **Resolved** state and the parent's resolution notes are added to each of them

- If you chose the incident to become the **Child**:

1. Select the parent to merge into and click **OK**.

2. The current incident will be moved to the **Linked to Parent** state while the parent moves along the workflow normally.

> **Note:** When you view the child, you will see a note about the item being merged and the parent item. The parent item is actually displayed on the **Parent Incident** tab of the child.

3. When the parent is resolved, the incident is automatically moved to the **Resolved** state and the parent's resolution notes are added to the incident.

3. Incident Investigation and Diagnosis

If the initial support fails to resolve the incident, the IT Service desk staff can transfer the incident to a Subject Matter Expert (SME). The SME investigates the incident, adds details, and, if possible, resolves the incident. Other options include escalating the incident to another SME or posting an RFC to the change management group.

The default incident management workflow contains three levels of support. Each level is associated with a different role as described below:

- **Investigation and Diagnosis** state – Incident Operator role

- **Escalated to L2** state – Level 2 Technician role

> **Note:** The **Level 2 Technician** selection list includes users who are in the *Level 2 Tech* and *Level 3 Tech* roles. This allows a Level 2 Tech to be selected to handle a lower level incident if the tech is available.

- **Escalated to L3** state – Level 3 Technician role

Depending on the state, the SME or technician can choose from the following actions:

- **Resolve** the incident, supplying how it was resolved and any other resolution details.

- **Escalate** the incident to the next level, for example, escalate the issue from level 2 to level 3.

- **Post RFC** to create a request for change from the incident. The incident moves to the **Pending Change** state. It will return to the **Investigation and Diagnosis** state after the related change is closed.

- **Post Problem** to either create a new problem or choose an existing problem (only available above level 2). To create a new problem, choose **Create New Problem** from the **Problem Link** drop-down list. To link to an existing problem, choose **Link to an Existing Problem** and search for the existing problem under **Raised**

Problem. The linked problem appears on the **Linked Problem** tab. The link can be removed by selecting **Remove Problem Link**.

> **Tip:** You can configure SBM to automatically assign the correct owner for each state. This improves the user experience by eliminating the need for them to select the correct SME when escalating the incident.

Similar to the **Classification** state, the investigation states allow the following additional actions to merge or create incidents:

- **Merge Incident** ties together the current incident with an existing incident using Parent/Child relationships. See Merging or Linking Incidents [page 52].

- **Copy Incident** creates a duplicate of the incident. You cannot modify the values when the item is created.

- **Post New Incident** creates another incident based on the current incident. You can modify the values in the new incident on the Submit form.

4. Incident Resolution and Closure

Incidents are resolved when service has been restored to normal. Incidents can be resolved in a variety of ways including attaching a Workaround or a Known Error. A *Workaround* includes the steps on how to circumvent the problem. A *Known Error* is a problem where there is no known fix. There may be a workaround for the Known Error or maybe not.

When resolving the error, you can select a Known Error, a Workaround, or a Knowledge Center article as a solution.

> **Note:** When the incident is resolved from the **Classification** state, the incident may be marked as **First Call Resolved**. This data is used in reports, such as **Weekly First Call Resolution Rate**, to keep managers informed to which incidents are resolved with the first call.

The option to create a **How To** article in the Knowledge Center is available on the Resolve transition. Selecting **Yes** will launch the submit form into Knowledge Management after completing the **Resolve** transition.

> **Restriction:** You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.

> **Note:** The content fields in the knowledge base article are automatically populated with the content from the incident. Selecting **Load Article Template** will erase the populated information, replacing it with the content from the template.

In the Resolved drop-down list, you can select Without Known Error, With Known Error, With Workaround, and With Knowledge Center article:

- **Without Known Error** enables you to enter the resolution details in the **Resolution** field.

- **With Known Error** and **With Workaround** enable you to search for existing known errors and their associated workarounds.

> **Tip:** When closing the item **With Known Error** or **With Workaround**, you must select a **Problem** or **Known Error** which is active. A problem cannot be selected if it is in the **Closed** state.

- **With Knowledge Center Article** enables you to search for and select a Knowledge Center article to associate with the incident. To search for the article, click **Search Knowledge Center** and choose the relevant article in the results.

Depending on whether the incident was resolved with a workaround:

- If the incident was resolved without a workaround, it moves to the **Resolved** state, where it can be closed.

- If the incident was resolved with a workaround, it moves to the **Resolved by Workaround** state. The incident remains in this state until the problem associated with the workaround is addressed. When the problem is closed, then the incident automatically moves to the **Resolved** state.

From the **Resolved** state, a user can close the incident by selecting the **Close** transition. The **Close** transition launches a Survey form, where users can rate their service desk experience. The survey form has four selection fields and a text entry field for additional comments.

The completed incident moves to the **Closed** state, indicating that it is no longer active. The final incident displays a total Survey Score, which is a summation of the weighted values of **Courtesy**, **Responsiveness**, **Technical Expertise**, and **Overall Satisfaction** values. The default weightings for **Courtesy**, **Responsiveness**, and **Technical Expertise** are the selected values. **Overall Satisfaction** is weighted at ten times the selection, for example, a selection of *1* would be weighted as *10* for the **Survey Score**. Change the weightings by editing the fields using SBM Composer.

> **Tip:** The **Satisfaction** dashboard provides four reports to assist in monitoring the responses to the satisfaction survey.

A second method of closing an incident from the **Resolved** state is the **IT Close** transition. This transition is available only to users in the IM Operators, IM Manager, IM Level 2, IM Level 3, and IM Administrator roles. This transition does not include a survey form.

> **Note:** If you are a member of IM User and a role with permissions to the **IT Close** transition, you will see two close transition buttons, **Close** and **IT Close**, on the **Resolved** state form. Choose the **Close** transition to complete the survey.

5. Incident Monitoring and Communication

Serena Service Manager has two main methods to monitor and communicate about the status of incidents: notifications and reporting.

The first method is through e-mail notifications, which inform users about the status of incidents. Automated e-mail notifications can be configured to notify users of incident creation, incident transfers, incident resolutions, and incident closures.

For example, you can create a notification that automatically informs incident submitters that they need to update their incident with more information. The submitters can either log in to the SBM User Workspace using the link in the notification or reply to the e-mail to update their incident.

The notifications are tailored using notification rules and notification templates. Administrators are responsible for editing the notifications and creating the workflow rules. See the *SBM Application Administrator Guide* for more information.

Users can subscribe to the selected notifications under their **User Profile** in SBM User Workspace.

For information on reporting, see the following section, 6. Incident Reporting [page 56].

6. Incident Reporting

In addition to the preconfigured reports that are included with the Service Manager, you can create a variety of reports in SBM to track your incidents.

The following are some example reports:

- First Call Resolution

- Mean Time to Incident Resolution

- Number of Incidents SLA Breaches per Week

- Number of Incidents by Category

- Number of Escalations

You can also combine reports to create a dashboard or multi-view report like the one created for the Incident Management launch page (Incident & Service Requests Dashboard [page 57]).

> **Tip:** You can create reports to perform keyword searches on auxiliary tables, such as the Workarounds table. To create this type of report, select to report on the Workarounds auxiliary table and create a search filter with `Title contains Query-at-runtime`. When you run the report, you will be prompted to enter your keyword search criteria, and the results will return all workarounds which contain the search terms in the title.

For details on creating and running reports, refer to the SBM User Workspace online help.

Incident Management Workflow

The Incident Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Classification* and *Major Incident*, and the transitions are marked with arrows, such as *Close* and *Assign*. The process starts with the **Submit** and can proceed along the different transition arrows.

The **Incident** workflow is one the workflows in the Service Desk Process App. The others are used for request fulfillment.

You can access this diagram through SBM Composer or SBM Application Administrator. Use SBM Composer to modify the workflow.
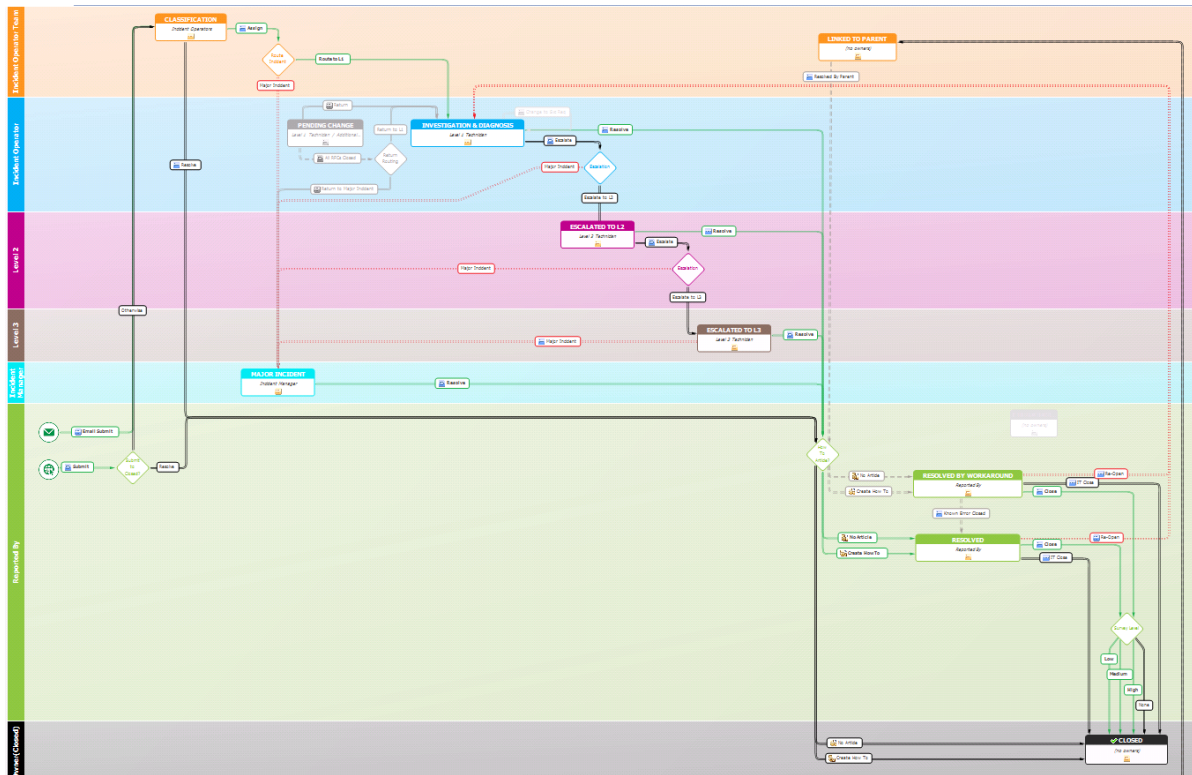
Incident & Service Requests Dashboard

The Incident & Service Requests Dashboard is designed to give managers and staff an overview of existing incidents and possible problem areas. The following screenshot and descriptions explain the information that the reports convey.

The Incident & Service Requests Dashboard report is available in the reports that are shipped with the Service Desk Process App snapshot.

Tip: Set the Incident & Service Requests Dashboard report as the home page report for the IT Services application by opening the **Service Desk** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.
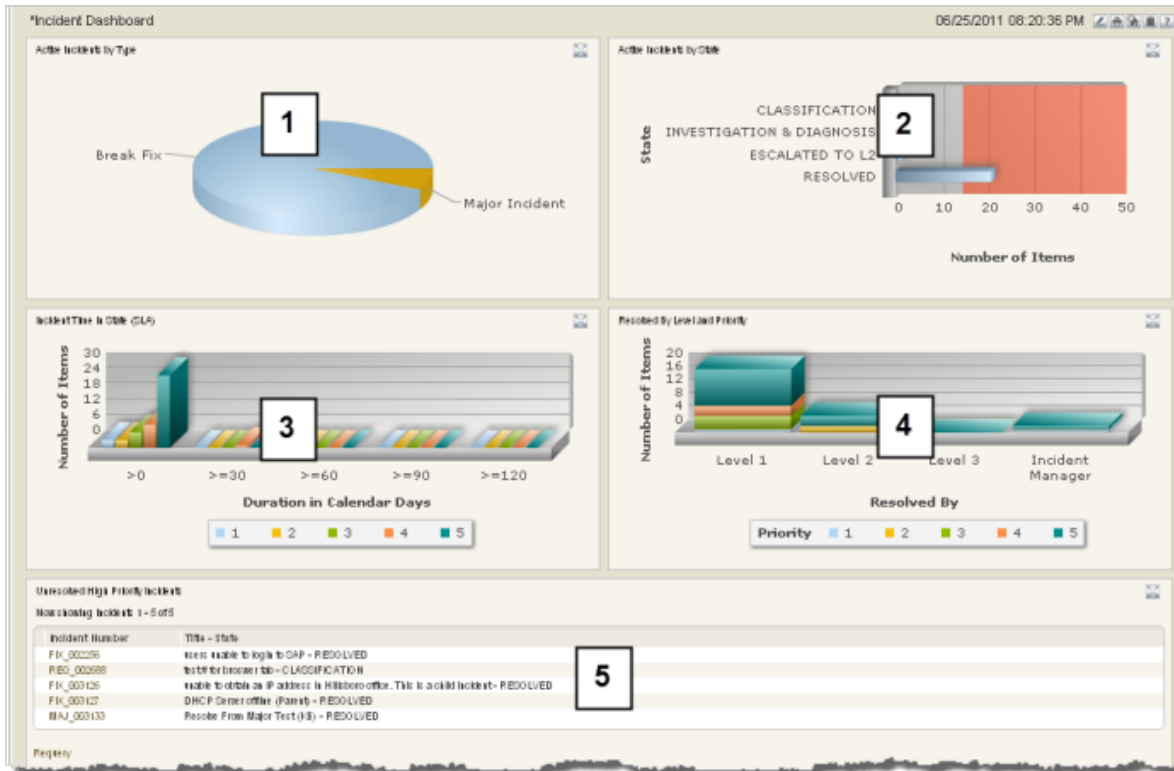
1. **Active Incidents/Service Requests by Type** gives an overall view of the distribution of incidents based on their type. Note that this report does not appear in the on-demand trial version of Serena Service Manager. Instead, there is a list of training videos to enable you to get up and running.

2. **Active Incidents/Service Requests by State** shows incidents and whether the number of incidents has reached a threshold. This graph allows the team to be proactive in addressing issues and keeping them under the critical threshold.

3. **Incidents/Service Request Time in State (SLA)** shows the duration of time that incidents remain in each state. Incidents are grouped by priority.

4. **Incidents/Service Requests Resolved by Level and Priority** shows at which support level incoming incidents have been resolved.

5. **Unresolved High Priority Incidents/Service Requests** lists existing high priority incidents. These incidents may be a cause for alarm because they are high priority yet have failed to be addressed.

> **Note:** The dashboard report is a multi-view report titled **Incidents/Service Requests Dashboard**. You can modify this report to add additional reports that help you to improve your Service Desk Process App. You can modify the report under the Report pane in the SBM User Workspace.

Satisfaction Dashboard

The Satisfaction dashboard is designed to give managers and staff an overview of how quickly incidents are being addressed and the responses to the satisfaction surveys for the incidents. The following screenshot and descriptions explain the information in the report.

The Satisfaction dashboard report is available in the reports that are shipped with the Incident Management snapshot.

Tip: Set the Satisfaction Dashboard report as the home page report for the IT Services application by opening the **Incidents** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.
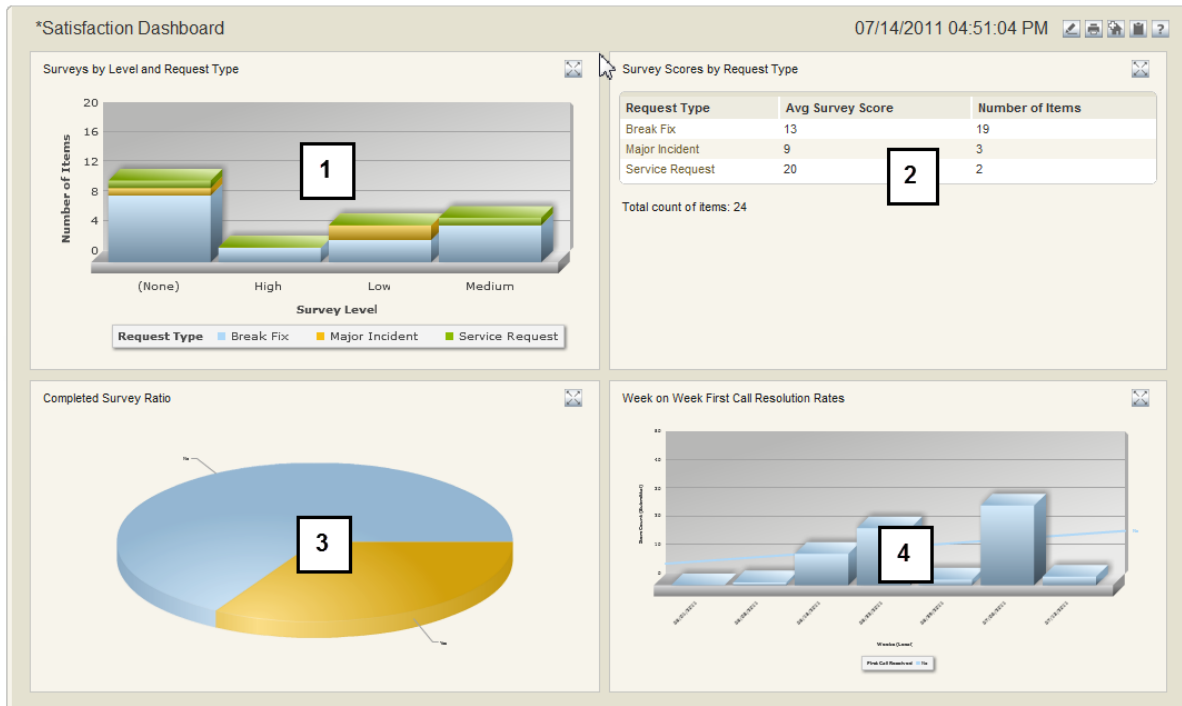
1. **Surveys by Level and Request Type** shows the incidents that have completed surveys based on level and type. You can drill-down to the incident to view the survey.

2. **Survey Scores by Request Type** shows the average score and the number of surveys that were received per incident type.

3. **Completed Survey Ratio** shows the number of incidents with completed surveys compared to the number of incidents where surveys were not completed.

4. **Week on Week first Call Resolution Rates** shows the number of incidents that were resolved on the first call, broken down by weeks.

> **Note:** The dashboard report is a multi-view report titled **Satisfaction Dashboard**. You can modify this report to add additional reports that help you to improve your Incident Management process. You can modify the report under the Report pane in the SBM User Workspace.

Incident Management Roles

The following roles (or actors) are used in the Incidents workflow.

> **Note:** The Incidents workflow and the request fulfillment workflows are in the Service Desk Process App. The Level 1 Techs role is used by all of these workflows.

Use the SBM Application Administrator to assign users to roles.

Incident Manager - The Incident Manager is responsible for the Incident Management/ Request Fulfillment process. Other duties include:

- Ensure efficiency and effectiveness of the Incident Management/Request Fulfillment process

- Manage Incident Management/Request Fulfillment staff

- Provide for continuous service improvement for Incident Management/Request Fulfillment

- Produce KPI reports for management review

- Maintain the Incident Management/Request Fulfillment system

- Collaborate with other Service Manager processes such as Request Fulfillment, Problem Management, Change Management, and Configuration Management

Level 1 Techs - This role is for service desk staff or first level support who are responsible for handling incoming calls and e-mails. The responsibilities of this role include:

- Own incidents/requests from recording to closure

- Record, classify, and resolve incidents/requests as quickly as possible

- Collaborate with end users and technical SMEs with the goal of quickly restoring normal service operation

- Escalate incidents/requests appropriately

- Keep end users informed of incident/request status

- Ensure Service Levels are met

- Match similar incident/request records

Level 2 Techs and **Level 3 Techs** - This role is for Technical SMEs and advanced support staff responsible for further incident investigation and diagnosis. Their other tasks include:

- Resolve incidents that were not resolved at First level

- Escalate service level breaches to Incident Manager

- Inform Service Desk staff of incident status and resolution

- Identify matching workaround

- Record new workaround

> **Note: Incident Operators** include all members in Level 1 Techs, Level 2 Techs, and Level 3 Techs.

Incident Users - This role is for the end users who will be submitting incidents, providing the necessary details to the Service Desk. IM User is the only role associated with the **Affected User** field.

Incident Contacts - This role is for the user accounts who should be available for selection in the **Additional Contacts** field.

IM Administrator - This role is responsible for administering Incident Management/Request Fulfillment, such as assigning users to roles or fixing SBM issues.

Chapter 6: Request Fulfillment

Note: Request fulfillment was added as a service operation in ITIL V3. The request fulfillment application is contained within the Service Desk Process App.

Request fulfillment is responsible for handling requests that are less than major changes and outside of items that require immediate resolution such as problems and incidents. These requests can come from employees or customers. Each request is logged and tracked as it progresses through the workflow. Request Fulfillment includes an approval process which must be completed before fulfilling the request.

Note: Service requests differ from incidents because they are not accompanied by a service interruption. In other words, there is nothing broken that needs fixing with a service request.

Typical service requests include:

- Configuration such as new employee setup or network access.

- Security requests such as allowing building access.

- Facilities requests such as moving offices or furniture.

- Communication requests such as adding a cellular phone.

- Information requests such as how to connect to the network.

The following topics describe the features found in Request Fulfillment:

Key Benefits

- Four different processes for tracking and monitoring requests.

- Reports for showing response time and customer satisfaction.

- Approval process to manage requests.

- Request fulfillment workflow according to ITSM best practices.

Request Fulfillment Overview

The Service Request application is contained within the Service Desk Process App. There are four different workflows with Service Request for request fulfillment.

Note: For the a dashboard report for request fulfillment, see

The following descriptions apply to all four workflows, except where noted:

1. Request Creation [page 64]

2. Request Classification and Initial Support [page 64]

3. Request Approvals [page 65]

4. Request Resolution and Closure [page 66]

5. Request Monitoring and Communication [page 66]

1. Request Creation

Request creation is known as submitting requests in Serena Service Manager. The primary actors responsible for submitting incidents are employees, customers, and IT Service Desk staff.

Employees and customers can submit their requests using the Request Center or SBM User Workspace. The following example describes submitting a request using Request Center.

> **Important:** The following procedure assumes that there is a configured service action called **Order Hardware** under the **Hardware** category. This service action is included in the sample services. You must promote ALL of the snapshots before logging in to Request Center for the sample data to be available.

To create a new request using Request Center:

1. Log in to Request Center: `http://`*serverName*`/tmtrack/tmtrack.dll?shell=srp`.

2. Select the **Employee Services** category on the **Catalog** tab.

3. Click the **New Hire Request** service action to open the submit request form. Note that you must click on the title.

4. Complete the wizard submit form.

5. Click **OK** to create the new request.

2. Request Classification and Initial Support

Request classification includes setting priority, performing request matching, and determining which approvals are needed.

In the **Classification** state, the Service Desk staff reviews the request and determines how the request should be handled. The following actions may be available to you for updating and routing the request. Your actual available actions depend on your role:

- **Assign** the request to a Level 1 Technician.

- **Update** the request with additional information.

- **Recategorize** moves the request to another project within Incident Management. Use this transition to change the Service Request to an Incident.

- **Delete Incident**, removing the request from the system.

- Choose an action from the **More Actions** drop-down, such as Send an E-mail.

When assigning the request or transitioning the request, the fields can be modified. The following describes the information to add in the fields, and how the information is used:

- Choose the **Type**, **Urgency**, and **Impact** from the drop-down lists. **Priority** is calculated automatically as described in Urgency, Impact, and Priority [page 17], but the value can be overridden.

- Choose a **Level 1 Technician** who will be responsible for resolving the request once the request has been approved. Note that the Level 1 Technician selection includes *Level 1 Techs*, *Level 2 Techs*, and *Level 3 Techs*.

- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.

Depending on the process workflow that you are using, set the following approval values in following fields:

- For the Service Request workflow, select whether the request requires **Financial Approval** or **Business Approval.** If financial approval is required, enter the **Cost Center** associated with the request.

- Select the **Financial Reviewer** and **Business Reviewer** if this request requires approval. The request will be routed to these users before being returned to the Level 1 Technician for implementation.

3. Request Approvals

The service request workflow has two levels of approval: financial approval and business approval. These two approvals help ensure that requests adhere to the company's fiscal goals and business rules. The primary roles responsible for these approving requests are Financial Approvers and Business Approvers.

The type of Service Request workflow determines the approvals required:

- **Atomic** - Business Approval

- **Composite** - No Approvals

- **Requisition** - Financial Approval

- **Service Requests** - Approvals depend on whether either the **Requires Business Approval** field or the **Requires Financial Approval** field are set to **Yes**.

The Service Request workflow used is usually determined by the type of request. For example, requesting access to a building or network usually does not have any financial cost, but there is usually a business approval process to ensure that this person should be granted access rights. Access types of request use the **Atomic** workflow.

In contrast, purchase requests require financial approval but probably not business approval. The purchase request for a new PC would use the **Requisition** workflow.

When a request is routed for financial or business approval, the selected financial approver or business approver can either approve or reject the request. If approved, the request moves to the **Fulfillment** state, where the Level 1 Technician is assigned the item and becomes responsible for resolving the approved request.

> **Tip:** To require both types of approval, use the Service Requests workflow, set the values for the **Requires Business Approval** and **Requires Financial Approval** field to **Yes**, and mark the fields as read-only for the project. All requests with these settings will be routed for approvals.

4. Request Resolution and Closure

The actual fulfillment of a request depends on the nature of the request. The service desk staff may be able to fulfill a request, or the request may need to be sent to an outside group for completion.

After the request has been approved, it moves to the **Fulfillment** state, where the assigned Level 1 Technician is responsible for overseeing the closure of the request.

There are different options available to the technician to complete the request. The technician can choose to:

- **Resolve** the request, completing the request and closing the issue.

- **Request Info**, which sends the request back to the submitter to gather more information about the request.

- **Post a Request for Change** to address the request. This opens an RFC in the Change Management workflow which will track the change. The request moves to the Pending Change state, where it remains until the RFC is completed. Once completed, the request returns to the **Fulfillment** state where the technician can close out the request. The related RFC can be seen on the **Linked RFCs** tab of the request.

- **Create a Task** to address the request. This opens a subtask in the Task workflow in Incident Management. The Task workflow is a simple workflow with two main states, **In Process** and **Closed**. The request stays in the **Fulfillment** state while the subtask is being completed. Examples of subtasks could include placing an order with a vendor or acquiring an access fob. Once the subtasks are completed, the request moves to the **Task Completed** state where the technician can close out the request. The subtasks related to the request can be seen on the **Subtasks** tab of the request.

Depending on the technician's privileges, the following transitions may also be available:

- **Recategorize** moves the request to another project within Incident Management. Use this transition to change the Service Request to an Incident.

- **Delete** deletes the request.

The completed request moves to the **Resolved** state.

5. Request Monitoring and Communication

Serena Service Manager has two main methods to monitor and communicate about the status of requests: notifications and reporting.

The first method is through e-mail notifications, which inform users about the status of requests. Automated e-mail notifications can be configured to notify users of request creation, request transfers, and request resolutions.

For example, you can create a notification that automatically informs request submitters that they need to update their request with more information. The submitters can either log in to Request Center using the link in the notification or reply to the e-mail to update their request.

The notifications are tailored using notification rules and notification templates. Administrators are responsible for editing the notifications and creating the workflow rules. (On-premise only)

Users can subscribe to the selected notifications under their **User Profile** in SBM User Workspace.

In addition to the preconfigured reports that are included with the Service Manager, you can create a variety of reports in SBM to track your requests.

The following are some example reports:

- Active Service Requests by State

- Active Service Requests by Type

- Request Elapsed Time by Type

You can also combine reports to create a dashboard or multi-view report like the Incident & Service Desk dashboard.

Request Fulfillment Workflows

There are four request fulfillment workflows in Service Desk Process App, along with the Incident Management workflow. There is the base Service Request workflow and three sub-workflows. One of the major differences in the workflows is the types of approvals required in each workflow.

The following list describes the differences in each workflow and examples of how they can be used.

- **Atomic** - This workflow is used for requests that require a business approval but not a financial approval. This workflow may be used for employee access or voice mail setup.

- **Requisition** - This workflow is used for requests that require financial approval for items to be purchased. There is no business approval step in this workflow. This workflow may be used for purchasing new laptops or new operating systems.

- **Composite** - The composite workflow is designed for requests that require external tasks to be completed before the request can be fulfilled, such as a new hire request which could entail creating a new access badge, setting up voice mail, and getting a computer ready. To post additional items or subtasks, add a **Subtask** transition. The **Subtask** transition runs between the **Fulfillment** and **Pending Change** state, and it will be responsible for creating an item in the other workflows. Update the All Closed transition to automatically occur once all subtasks are closed.

- **Service Requests** - This workflow contains both a business approval and a financial approval step. The default workflow routes items based on the values in the

Requires Financial Approval and **Requires Business Approval** fields. Use this workflow for large scale purchases which will require both financial and business approvals, such as mainframe server or software purchases.

> **Note:** These workflows are demonstrated if you have installed the Starter Pack Forms. The sub-projects under Service Requests reference make use of these different workflows, as well as providing a special submit form for each project. See About Starter Pack Forms [page 41] for information about the different projects and where the workflows are used.

Use SBM Composer to modify the workflow or to view the workflow diagram.

Request Fulfillment Roles

The following roles (or actors) are available for the Service Requests workflow.

> **Note:** The Incidents workflow and the request fulfillment workflows are in the Service Desk Process App. The Level 1 Techs, Level 2 Techs, and Level 3 Techs roles are used by all of these workflows.

Use the SBM Application Administrator to assign users to roles.

Level 1 Techs - This role is for service desk staff or first level support who are responsible for handling incoming calls and e-mails. The responsibilities of this role include:

- Own incidents/requests from recording to closure

- Record, classify, and resolve incidents/requests as quickly as possible

- Collaborate with end users and technical SMEs with the goal of quickly restoring normal service operation

- Escalate incidents/requests appropriately

- Keep end users informed of incident/request status

- Ensure Service Levels are met

- Match similar incident/request records

Level 2 Techs and **IM Level 3 Techs** - In Request Fulfillment, these roles are included as Incident Operators, and members of the roles can be selected as owners for the initial classification of a request.

> **Note: Incident Operators** include all members in Level 1 Techs, Level 2 Techs, and Level 3 Techs.

Business Approvers and **Financial Approvers** - These roles are for the business and financial approvers who are responsible for verifying that a request meets the business and financial requirements.

Purchaser - This role is used in the **Requisition** workflow. The purchaser role is for users who will be responsible for the actually purchasing of the software or hardware.

Incident User - This role is for the end users who will be submitting requests, providing the necessary details to the Service Desk. Request User is the only role associated with the **Affected User** field.

IM Administrator - This role is responsible for administering Incident Management/ Request Fulfillment, such as assigning users to roles or fixing SBM issues.

Chapter 7: Problem Management

Problem Management is a deeper dive into the cause of incidents. Problem Management seeks to find a resolution to the root cause of a problem so as to minimize or prevent the recurrence of incidents caused by the problem. It seeks to identify known errors and define a resolution. This information can prevent service disruption in the future. Proactive Problem Management helps your team to decrease the number of incidents as trends are analyzed and permanent fixes are implemented.

Problem Management works together with Incident Management and Change Management to ensure that IT service availability and quality are increased. As permanent resolutions are found to fix known errors, Requests for Change (RFCs) can be raised to make alterations to your IT process, applications or infrastructure. As these RFCs are implemented to resolve problems, related incidents are less likely to occur.

Problems can be related to incidents, changes, or solutions, giving your support desk the information that they need when they encounter similar issues. Known Errors and their resolutions are added to the Knowledge Base, where they can be accessed by the support staff to help identify permanent solutions and speed up the resolution time of similar incidents. This results in less downtime and less disruption to business critical systems.

The following sections describe the Problem Management application:

- Problem Management Overview [page 71]

- Problem Management Workflow [page 75]

- Problem Management Dashboard [page 76]

- Problem Management Roles [page 77]

Key Benefits

- Problem management for root cause analysis.

- Ability to relate existing Known Errors to new problems.

- Automatic recording of Known Errors.

- Auxiliary table to store Workarounds.

Problem Management Overview

The problem management application contains the following areas:

1. Problem Creation [page 72]

2. Problem Classification [page 73]

3. Problem Investigation and Diagnosis [page 73]

4. Problem Error Assessment [page 74]

5. Known Errors [page 74]

1. Problem Creation

Creating a problem is known as submitting a problem in Service Manager. Problems may be submitted directly by the problem management staff or they may be spawned from an incident using the **Post Problem** transition in the Incident Management workflow.

The Submit form enables you to add the following information when creating a problem:

- **Problem Title** and **Problem Description** in the *Overview* section

- **Urgency**, **Impact**, and **Priority** in the *Problem Type* section. *For details, see* *Urgency, Impact, and Priority [page 17]*.

- **Primary CI**, **Problem Category**, **Sub-Category**, and **Sub-Category Type** in the *Configuration Item* section. *The Problem Category fields will populate based on the values in the Primary CI, but they can be modified. For details on CIs, see* *Configuration Management Overview [page 93]*.

- **Reported By**, **Affected User** and **Additional Contacts**. *The Reported By field is used when the submitter of the item is not the one affected by the issue.*

- Under Details, indicate whether a **Tech Note** should be created when the problem is resolved, and add **Work Notes** or **Attachments**.

- **Linked Incidents** tab allows you to link related incidents.

> **Note:** When the problem is created from an incident using the **Post Problem** transition, details from the incident are pre-populated into the Submit form.

To create a problem directly:

1. Select the **Problem** Application tab.

2. On the **Submit** navigation pane, click **Submit to My Preferred Projects**.

3. Select the project to submit into.

> **Note:** You will only be allowed to submit into a project if you have the appropriate permissions.

4. Complete the Submit form with the necessary information.

5. Click **OK** to create the new problem.

> **Tip:** You can find the items that you submitted by using Search by Submitter functionality and searching for items submitted by *Current User*.

When the problem is created, it is assigned a unique item ID and moves to the **Classification** state where it can be classified by the project management staff.

If you selected a configuration item (CI) for the problem, the **Active Problems** tab will show all active problems related to the particular CI and the **CI Relationships** tab will list all of the relationships for the particular CI.

2. Problem Classification

Problem classification involves the triage and assignment of the problem for more investigation. After a problem is submitted, it moves to the **Classification** state, where the project management team can choose to do one of the following:

- Choose to **Investigate** the problem.

- Choose to **Update** the problem with new information.

- Choose to put the problem on **Hold**.

- Choose to **Delete** the problem (option appears if user has the delete item privilege).

- Attach a file to the problem by clicking **Add File** under *Details* or selecting **Add File** from Item Action drop-down.

- Choose an Item Action such as Send an E-mail for the Actions.

- Relate incidents to the problem.

  Note: When you choose to relate incidents to the problem, the selected incidents are linked to the problem record, and the problem record is saved. On the **Related Incidents** tab, the related incidents records that were linked are shown.

3. Problem Investigation and Diagnosis

The **Investigation and Diagnosis** state is where the technical SME can investigate the root cause of the problem. The **Technical SME**, who is assigned the problem for investigation, is chosen when you select to **Investigate** the problem from the Classification state.

The Investigate transition lets you attach any necessary supporting documentation or add work notes to the file, supplying the additional information to the SME.

The SME will make use of Serena Service Manager to help diagnose and resolve the problem. **CMS** will be used to help determine the level of impact and to assist in pinpointing the point of failure. The **Known Errors** will be accessed and checked in order to discover whether the problem has occurred in the past, and if so, whether a resolution is already in place. Related problems should be checked to see whether similar problems have been raised previously. Information in these tables is available through the **Active Problems**, **CI Relationships**, and **Linked Incidents** tabs for the problem.

The result of an investigation for a problem will be a root cause diagnosis. The resolution should be the sum of the appropriate level of resources and skills used to find it.

Once the cause of the problem is discovered, it is forwarded to the **Error Control** phase. The information discovered about the cause is entered in the **Work Notes** field.

In addition to entering a root cause, the SME can perform one of the following actions in the *Investigation and Diagnosis* state:

- Choose to **Update** the problem with new information.

- Choose to put the problem on **Hold**.

- Attach a file to the problem by clicking **Add File**.

- Choose an Item Action such as Send an E-mail for the Actions.

4. Problem Error Assessment

Once the causes of a problem have been discovered, the problem goes into the Error Control phase, which is when a resolution to the known error is established. The Error Assessment state is when the SME logs the known error and describes a workaround.

The SME selects the **Error Identified** transition to log the Known Error and workaround. This transition allows the SME to add the details about the Known Error and what the workaround would be. The SME enters information for the Known Error under the **Known Error Notes** field.

> **Note:** The **Error Identified** transition changes the problem prefix to KE, signifying that it is a Known Error. Known Errors are described in the following topic.

After completing the Error Identified transition form, a **Workaround** submit form is displayed, where the SME can enter information about the workaround for the problem. Workarounds are submitted into the **Workarounds** auxiliary table. The items are linked to the problem. This allows incidents that are linked to the problem to be able to refer to the workaround.

> **Note:** You can avoid submitting the workaround at this point and add it in the next state. To avoid submitting a workaround at this time, click **Cancel** on the Workaround Submit Form.

In addition to transitioning the item and adding a workaround, the SME can choose from the following actions in the **Assessment** state:

- Choose to **Update** the problem with new information.

- Choose to put the problem on **Hold**.

- Attach a file to the problem by clicking **Add File**.

- Choose an Item Action such as Send an E-mail for the Actions.

5. Known Errors

In ITIL terminology, when the root cause of a problem is known and there is a workaround, it becomes a **Known Error**. Serena Service Manager changes the problem to a Known Error record automatically during the **Error Identified** transition.

The change from problem to Known Error is noted by the change of the Problem ID prefix from PR to KE. This change allows users to easily discern problems from known errors when looking at a Problems report, such as the report that is displayed on the **Problems** tab for a configuration item. You can also create a report that searches only for items that have a **Problem Type** of Known Error to help find possible solutions.

6. Problem Resolution

Problems can be resolved in a variety of ways. First, there may be a workaround to the problem, explaining how to address the problem when it is encountered. Second, the problem may be caused by an underlying problem in the system that needs to be changed. A change needs to be made in the system at large to fix the root cause of the problem. And third, the problem may have no solution and will have to be lived with. In

this case, you may want to create a tech note in Knowledge Center to alert people about the problem.

These three ways are not mutually exclusive; for example, there may be a workaround but there may still be a problem in the system that needs to be resolved.

> **Tip:** A good practice is to occasionally review all major problems to ensure that the correct steps were followed, how to improve the process overall, and how to prevent recurrence of similar incidents. The reporting functionality in SBM helps to expedite this review process. You can create and share reports listing the major problems that were recently closed, and then share the list with your team.

All three of these approaches may be implemented from the **Error Identified** state in the problem workflow:

- **Add Workaround**, which opens a Submit form into the Workaround auxiliary table.

- **Post RFC**, which opens to the Submit form into the Changes workflow. This change is linked to the item. The problem moves into the Pending Change state. It will be automatically transitioned back to the **Error Identified** state when the change is completed.

- **Resolve**, which moves the known error to the **Resolved** state, where it can be reassessed at a future time.

  To create a tech note from the problem, select **Yes** to **Create Tech Note** field. The tech note will be created when the problem is closed with the **Close** transition. The Close transition will open a submit form into Knowledge Management.

  > **Restriction:** You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.

  > **Note:** The content fields in the knowledge base article are automatically populated with the content from the problem. Selecting **Load Article Template** will erase the populated information, replacing it with the content from the template.

Problem Management Workflow

The Problem Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Classification* and *Assessment*, and the transitions are marked with arrows, such as *Investigate* and *Hold*. The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM Application Administrator. Use SBM Composer to modify the workflow.
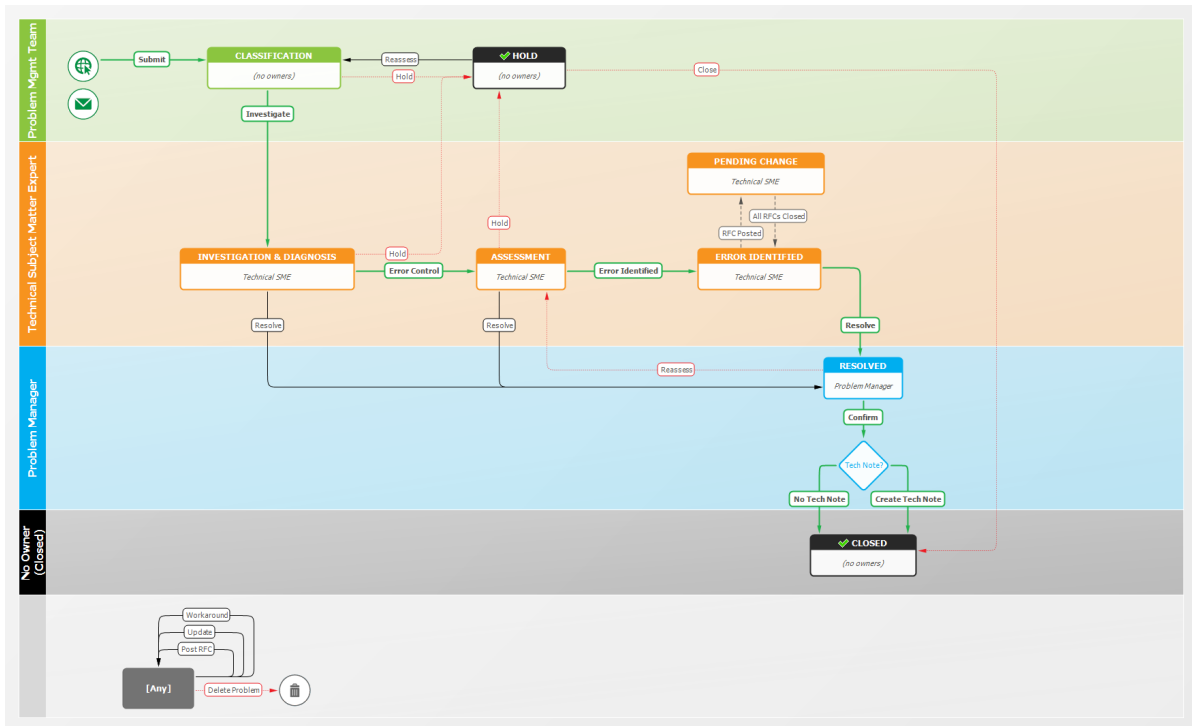
Problem Management Dashboard

The Problem Management dashboard is designed to give managers and staff an overview of existing problems, which states they reside in, what the backlog of problems is, and what the high priority problems are.

The **Problem Dashboard** report is available in the reports that are shipped with the Problem Management snapshot.

> **Tip:** Set the Problem Dashboard report as the home page report for the Problem Management application by opening the **Problems** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.
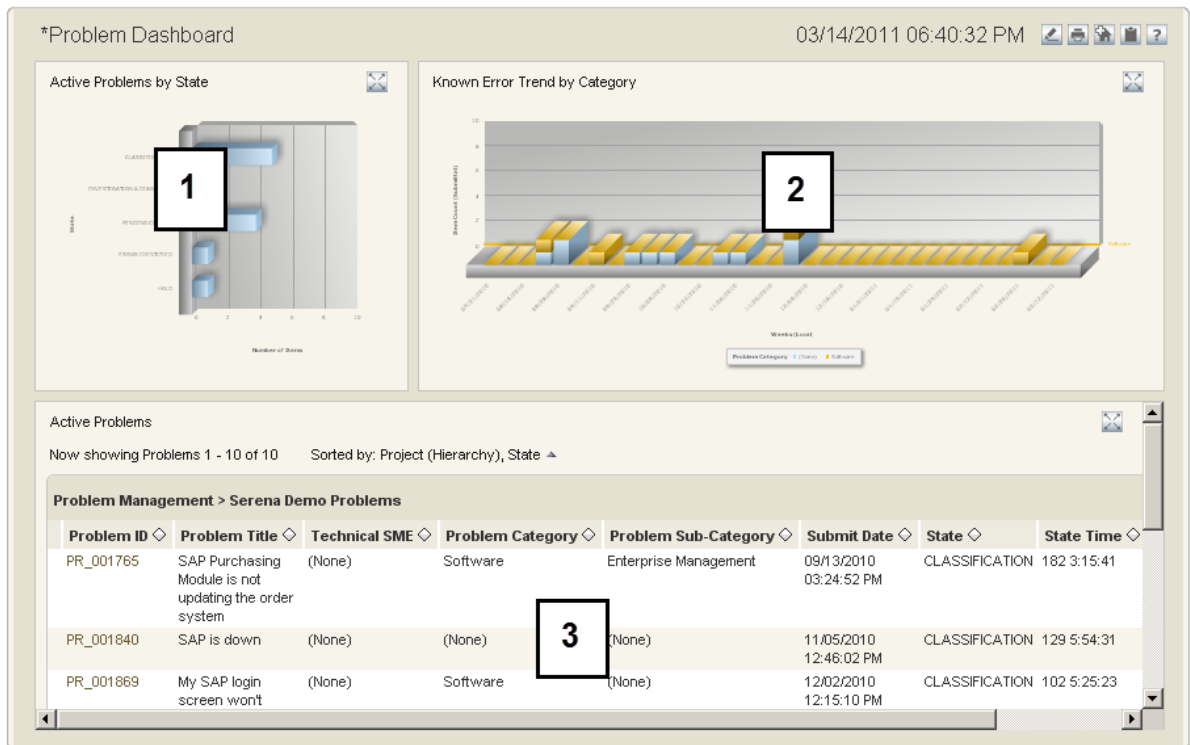
1. **Active Problems by State** shows problems that have not been resolved. The problems are broken down by state. This graph allows the team to see where in the problem management process most problems are.

2. **Known Error Trend by Category** is a graphical trend report, showing the submittal rate of problems over the recent time frame. The submittal rates are divided based on the category of the problem.

3. **Active Problems** lists all problems in active states, such as CLASSIFICATION, ASSESSMENT, INVESTIGATION & DIAGNOSIS, and PENDING CHANGE.

> **Note:** The dashboard report is a multi-view report titled **Problem Dashboard**. You can modify this report to add additional reports that help you to improve your Problem Management process. You can modify the report under the Report pane in the SBM User Workspace.

Problem Management Roles

The following roles (or actors) are available in the Problem Management process app. Use the SBM Application Administrator to assign users to roles.

Problem Manager - The Problem Manager is responsible for the Problem Management process. Other duties include:

- Ensure efficiency and effectiveness of the Problem Management process

- Initiate proactive Problem Management initiatives

- Provide for continuous service improvement for Problem Management

- Monitor the quality and usefulness of problem records and known error information

- Produce KPI reports for management review

- Maintain the Problem Management system

- Collaborate with other Service Manager processes such as Incident Management, Change Management, and Configuration Management

Problem Specialist - This role is for Technical SMEs and advanced support staff responsible for problem investigation and diagnosis. The responsibilities of this role include:

- Perform investigation and diagnosis to determine the root cause of problems

- Identify, record, and update known error record

- Identify incident trends that might be caused by a technical error

Problem Staff - This role provides information to problem management staff as needed, including technical and business related details.

Problem Submitters - This role is problem submitters who are responsible for providing incident details to Problem Management staff.

PM Administrator - This role is responsible for administering Problem Management, such as assigning users to roles or addressing SBM issues.

Chapter 8: Change Management

Change Management helps ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure. This minimizes the number and impact of any related incidents upon service operations after changes are implemented.

The Change Management process included with Serena Service Manager is designed to be flexible so that you can tailor the process to your environment. It includes only the basic states, expecting that you will add states and transitions to meet your needs. The default workflow includes basic states such as Classification, Assessment, CAB Review (Change Approval Board), Approved Changes, Implementation, Post Implementation Review, and Successful.

> **Important:** The **Link Release Train** transition is only applicable if you have Serena® Release Manager (SRM). To eliminate confusion and possible problems, administrators should disable this transition if SRM is not installed.

Key Benefits

- Flexibility in implementing tailored change management processes.

- Ability to spawn Requests for Change from problems.

- RFC path through workflow determined by Category Type.

Change Management Overview

The change management application addresses the following areas:

1. RFC Creation

Creating a request for change (RFC) is known as submitting in Serena Service Manager. Requests for change may be submitted directly into the change management process or from another management process using the **Create RFC** transition.

> **Tip:** Automated raising of an RFC when a CI is updated can also be enforced.

When creating an RFC, you add information about the RFC by completing the Submit form. The form contains multiple fields and tabs to enter appropriate information, such as:

- Change Title and Description

- Change Type and Category

- Urgency, Impact, and Priority (For details, see Urgency, Impact, and Priority [page 17].)

- Primary CI

    Note: When you select a configuration item on the submit form, a new baseline is created automatically in CMS for the configuration item. This process uses the **Create CI Baseline** submit path on the Change Management workflow. See Understanding Baselines [page 98] for more information.

- Contact Details

- Announce Change

- Risks

- Communication, Training, and Marketing Plans

- Implementation Plans

- Linked CIs, Problems, and Incidents

    Note: If the RFC was created from an incident or problem, the details are pre-populated into the RFC.

To create an RFC directly:

1. Select the **Changes** Application tab.

2. On the **Submit** navigation pane, click **Submit to My Preferred Projects**.

3. Select the change management project to submit into.

    Note: You will only be allowed to submit into a project if you have the appropriate permissions.

4. Complete the Submit form with the necessary information.

    Note: You can modify the workflow to select which fields are mandatory at each step of the process. For example, the default workflow requires that the submitter selects Change Type and Priority. Your process may require that the Change Manager sets these values when assessing the RFC. You can modify the workflow accordingly.

5. Click **OK** to create the new RFC.

When the RFC is created, it is assigned a unique item ID and moves to the **Classification** state where the change manager will determine how the change will be addressed.

    Tip: You can find the items that you submitted by using Search by Submitter functionality and searching for items submitted by *Current User*.

2. RFC Classification

Once the RFC has been created, a preliminary assessment needs to be made of its importance. This occurs when the item is in the **Classification** state.

All fields are available for editing when you are updating or transitioning an item from the **Classification** state. This allows the change manager to modify the proposed values for priority, urgency, and category type that were selected by the submitter.

The change manager must determine what type of change the RFC is. The **Change Type** value controls which paths are available for the change to take through the workflow. For "standard" changes, the change manager can choose to **Pre-Approve** the change. In ITIL, "standard" changes refer to those changes that are commonly performed, such as password resets or user account provisioning. These "standard" changes are pre-approved, and therefore there is no need to go through the normal approval process. The changes skip the CAB and move directly from the *Classification* state to the *Approved Changes* state. For regular changes, the change manager selects the **Normal** type. Normal changes move through the entire workflow. The **Emergency** change bypasses the *Assessment* state and moves directly to the ECAB (Emergency CAB), which is a subset of the CAB. ECAB is convened to handle emergency RFCs.

> **Tip:** Emergency changes must be responded to immediately, and the procedure to be followed in such cases must be planned for. It is possible to create a notification in SBM to inform ECAB members about Emergency RFCs that must be responded to immediately.

From the **Classification** state, the change manager can choose from a variety of options, depending on the value of the Change Type:

- An RFC may be *accepted*, which does not mean that it will subsequently be approved by the CAB, only that it is sufficiently justified to be given further consideration.

- An RFC may simply be *rejected* if it is felt that the change is not justified.

- An RFC may be *deferred* back to the originator, who can modify the item and then *re-open* it after the change is defined more clearly.

- An RFC may need to be *assessed* further by the change manager before being sent to the CAB.

- A pre-approved RFC can be *implemented* immediately without moving to the CAB.

> **Note:** If the RFC was not submitted with linked items, the **Linked Items** tab does not appear on the **Classification** state form. The change manager must select to **Update** to add linked items such as problems, incidents, or other CIs.

3. RFC Assessment

A preliminary assessment occurs in the **Classification** state when the change manager determines the change type and where to route the change; however, a deeper assessment may be required. When this is the case, the change is routed to the **Assessment** state where a change manager can further assess the change.

When assessing the RFC, the change manager needs to set the appropriate values for the priority and category. Priority and Change Category are important settings for the RFC process in ITIL. The *Priority* determines the relative importance of the RFC in relation to other outstanding RFCs and it should be the main basis of when pending changes are

scheduled. The Change Category determines the difficulty and impact of the RFC and will be the main parameter used to determine the resources that need to be allocated. The default Change Category types are:

- Minor

- Significant

- Major

Assessment also involves calculating the possible risk in implementing the change. The Risk Calculator on the **Risk** tab automatically determines the risk based on the change category, estimated effort, and an array of survey questions. For more information, see Risk Analysis Calculator [page 82].

Following assessment, the change manager **accepts** the RFC, and the RFC transitions to the Change Approval Board (CAB) for approval.

> **Note:** Financial and Effort estimates are required for items that go through the Assessment phase.

Risk Analysis Calculator

The Risk Analysis calculator determines how the change affects business critical services. The Risk Calculator uses the change category, the estimated effort, and a group of questions to determine the risk level of the change.

The Risk Analysis calculator appears on the **Risk** tab of an RFC. The risk level is determined to be either **Low**, **Medium**, or **High** based on the weighted answers to the survey questions, the change category, and the estimated effort. The default ranges are: **Low** is less than or equal to 20; **Medium** is 21 to 40; **High** is greater than 40.

> **Note: Total Risk Score** contains the summation of the weighted answers to the survey.

On the **Risk** tab, the risk level only displays when the **Risk Analysis Completed** field is set to **Yes**. This ensures that users have answered the risk survey before calculating the risk level. If the risk survey has not been completed and **Risk Analysis Completed** remains set as **No**, the risk level displays **Questionnaire Not Completed**.

> **Tip:** When creating a report to show high risk items, remember to include both items which have a high **Total Risk Score** and items which have a change category set as **Major** and their **Risk Analysis Completed** field set as **No**. Items without a completed risk survey will show a lower overall risk level since the risk level sums the survey responses and a null response is given a weight of zero.

The following are the default questions and weighted answers (default weights) in the Risk Analysis questionnaire:

1. **Does the change affect business-critical services?**

   - High Impact: Service temporarily unavailable / major changes (10)

   - Low Impact: Small upgrade, some features temporarily unavailable (5)

   - No Impact (0)

2. **Does the change affect major IT infrastructure components?**

    - High Impact: Components taken offline / major service impact (10)

    - Minor upgrade or temporary performance degradation (5)

    - No Impact (0)

3. **Will the change be tested prior to implementation in a development or test environment?**

    - Yes (3)

    - No (7)

4. **Is the implementation well understood and documented?**

    - This process has been done in the past and is repeatable (0)

    - This process is similar to one done in the past (5)

    - This is a completely new process or implementation (10)

5. **What is the implementation time?** *This field is set automatically based on the value entered in the Estimated Effort field for the change request. It can also be manually modified by choosing a selection in the list. The Estimated Effort field appears on the Implementation tab for a change request. This tab appears when approving a change.*

    - 4 hrs or less (0)

    - 4 hrs to less than 1 day (5)

    - More than 1 day (10)

6. **What is the change complexity?** *This field is set automatically based on the value of the Change Category.*

    - Minor (0)

    - Significant (5)

    - Major (10)

Modifying the Risk Calculator and Survey

You can modify the risk calculator and survey so that it reflects your company's processes. This topic describes how you would modify the calculator and survey.

The Risk Calculator uses a summation field to add the values of the weighted selections. The summation value is then evaluated using a JavaScript which adds a risk level of either **Low** (0-20), **Medium** (21-40), or **High** (>40).

The Risk Level is configured to only display a result when the **Risk Analysis Completed** binary field is set to **Yes**. This field is automatically updated by a JavaScript to **Yes** if any of the four survey fields contain an answer. After being set to **Yes**, the weighted values are summed and the results displayed. If not, the Risk Level displays **Questionnaire Not Completed**.

You can modify the risk survey and calculator, such as the risk level thresholds, the questions, or the weightings of the answers. The modifications are performed within SBM Composer, and then the changes are deployed to your server.

The following are some changes that you could make to the survey:

- Make the survey mandatory by marking all of the fields as **Required**.

- Modify the weighted responses to questions by selecting to edit the field and setting the weighted values on the **Options** tab of the **Property Editor** for the field.

- Change existing questions and answers by modifying the field names and descriptions in the **Property Editor** for the field.

- Add new questions by adding single selection fields with weighted values. To add the new questions, you must:

  - Modify the summation field (**Total Risk Score**) to include the weighted value in the result.

  - Add the new field to **Risk** tab on every form in the Change Management process application.

  - Add the field name to the JavaScript contained in the **calcRisk_Transition** HTML/JavaScript widget. This script is responsible for checking if the question is answered. The following example of how you would add a new field is an excerpt of the JavaScript:

```
AddChangeCallback("ESTIMATED_EFFORT", funcLinkEstimatedEffort);
AddChangeCallback("RISK_ANALYSIS_Q1", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q2", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q3", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q4", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q5", funcAnalysisCompleted);
AddChangeCallback("NEW_FIELD_NAME", funcAnalysisCompleted);
```

- Change the range for how risk is calculated by editing the JavaScript on the state forms. The JavaScript is contained in the **calcRisk_State** HTML/JavaScript widget. For example, you would make the following change to add an additional risk category for Medium-High for risk scores between 31 and 40:

```
<script type="text/javascript">
AddLoadCallback(calcRisk);
function calcRisk() \{
var answered = GetFieldValue("RISK_ANALYSIS_COMPLETED");
if(answered == "Yes") \{
var score = parseInt(GetFieldValue("TOTAL_RISK_SCORE",  0));
if(score > 40) \{ SetFieldValue("RiskScoreLabel", "(High Risk)"); }
else if( score > 30) \{SetFieldValue("RiskScoreLabel", "(Medium-High Risk)"); }
else if( score > 20) \{SetFieldValue("RiskScoreLabel", "(Medium Risk)"); }
else \{ SetFieldValue("RiskScoreLabel", "(Low Risk)"); }
\}
else \{
SetFieldValue("RiskScoreLabel", "(Questionnaire Not Completed)");
\}
```

```
\}
</script>
```

- Change how the estimated effort is weighted by modifying the JavaScript on the transition forms. The JavaScript is contained in the **calcRisk_Transition** HTML/ JavaScript widget. For example, to set everything under 1/2 day (12 hours) as low impact and everything else as high impact:

```
<script type="text/javascript">
var funcLinkEstimatedEffort = function()\{
        var effort = GetFieldValue("ESTIMATED_EFFORT", "");
        var implTimeFld = GetFieldByName("RISK_ANALYSIS_Q5");

        if(effort != "") \{
        //Convert Estimated Effort field from milliseconds to hours
                var hours = effort / 3600000;

                if(hours > 12) \{ implTimeFld.selectedIndex = 3; \}
                else \{ implTimeFld.selectedIndex = 1; \}

                DisableField("ESTIMATED_EFFORT");
        \}
\}
```

For more information on working with fields, refer to the *SBM Composer Guide*.

4. RFC Authorization

Information management systems are highly sensitive to configuration changes due to the complex relationships between all the CIs involved. An apparently minor change may trigger a chain reaction with catastrophic results. The **Change Advisory Board** (CAB) is responsible for evaluating the changes and discussing the possible side-effects of the change before giving their approval.

The CAB is usually chaired by the change manager, and its members include other service management managers. The CAB may also include other stakeholders such as customers or other third-party providers. In the case of high impact changes, upper management may need to be consulted as strategic issues and the organization's general policy may come into play.

> **Note:** The default change management workflow assumes that the CAB would be conducted offline, and the change manager would then approve the RFC on behalf of the CAB. The default workflow can be modified to allow individual CAB approvals. One approach to allow individual approvals is to use the subtasking capabilities of SBM. Subtasks can be created and assigned to each selected CAB member, and then they can approve or reject the individual tasks, and the results can be displayed in the parent RFC.

The CAB must meet regularly to analyze and approve the pending RFCs. The members discuss the benefits of the RFC and verify that a back-out plan exists in case the change does not work as expected. They decide the date of when the RFC should be implemented, assess the effort, and assess the cost.

The CAB also discusses possible risks, services that are affected, impacts to business continuity, and disaster recovery. The results and decisions of the discussion should be

collected and entered in the RFC. The details can be entered directly into the text fields or they can be attached as supporting documentation using **Add File**.

> **Tip:** Once the change has been approved, it can be assessed whether it should be implemented in isolation or as part of a package of changes that would be formally equivalent to a single change. This approach optimizes the use of resources, reduces the incompatibilities between different changes, and simplifies the back-out plan. Change managers can link RFCs by creating a principle RFC and then grouping the RFCs together using the subtasking capabilities of SBM.

Announcing a Change

The option to **Announce Change** enables you to post an Announcement to Knowledge Management after completing the **Approve** transition from **CAB Review**.

When **Announce Change** is set to **Yes**, the submit form into Knowledge Management will display after completing the **Approve** transition.

The content for the new Announcement will be populated with information from the article. The start date for the *Announcement* is set to the *Implementation Start Date* from the change.

> **Restriction:** You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.

> **Note:** Selecting **Load Article Template** on the **Content** tab will erase the information that was imported from the change. The content will be replaced with the template.

5. RFC Implementation

The responsibility for implementing a change usually falls in the realm of the Release Management; however, the Change Management team remains responsible for overseeing and coordinating the implementation of the changes. The change management team usually helps to monitor that:

- Schedules are met and the appropriate resources are assigned.

- Software is developed and hardware is purchased according to specifications.

- The test environment is realistic and simulates the live environment.

- Back-out plans are created that will allow the last stable configuration to be recovered rapidly.

The default Change Management workflow is designed with the assumption that implementation steps vary between companies, and that the steps would be tailored according to the company's processes. The workflow contains only one state, **Implementation**, where the *Implementer* is assigned as the primary owner and the *Implementation Team* acts a secondary owner.

This process can easily be enhanced to meet your needs. Here are some examples:

- Add additional states to the change management process to track the implementation steps.

- Link the change management process to your existing release management process using Web services.

- Use subtasks to track the implementation tasks, automatically transitioning the RFC when the subtasks are complete.

After the implementation is complete, the RFC moves to the Post Implementation Review state, where the change manager conducts a review of the RFC before closing it.

6. RFC Review and Closure

After the implementation is complete, the RFC moves to the **Post Implementation Review** state, where the Change Manager can conduct a review of the change. This is known as a Post Implementation Review (PIR).

> **Note:** By default, the Change Manager is notified when a change is transitioned to the Post Implementation Review state.

The review allows the real impact of the change on the organization's quality of service and productivity to be assessed. Some of the basic points to take into account are:

- Were the objectives met, and if necessary, were there any restrictions?

- Did the process deviate from the original plans?

- Were there any unexpected problems?

The PIR also verifies that all of the information related to the implementation is entered into the Change Record, such as the Objectives, Beginning and End dates, Time and Effort, Cost, and Lessons Learned.

If the final evaluation finds the process and results to have been satisfactory and the information entered in the RFC, the RFC can be closed using the **Complete** transition.

Items that raised the RFC are automatically transitioned to the next state when the RFC is closed. For example, if the RFC was raised from a problem, moving the problem to the Pending Change state. When all of the RFCs are closed, the **All RFCs Closed** transition is automatically performed, moving the problem back to the **Assessment** state.

Change Management Workflow

The Change Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Deferred* and *CAB Review*, and the transitions are marked with arrows, such as *Reject* and *Accept*.

The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM Application Administrator. Use SBM Composer to modify the workflow.
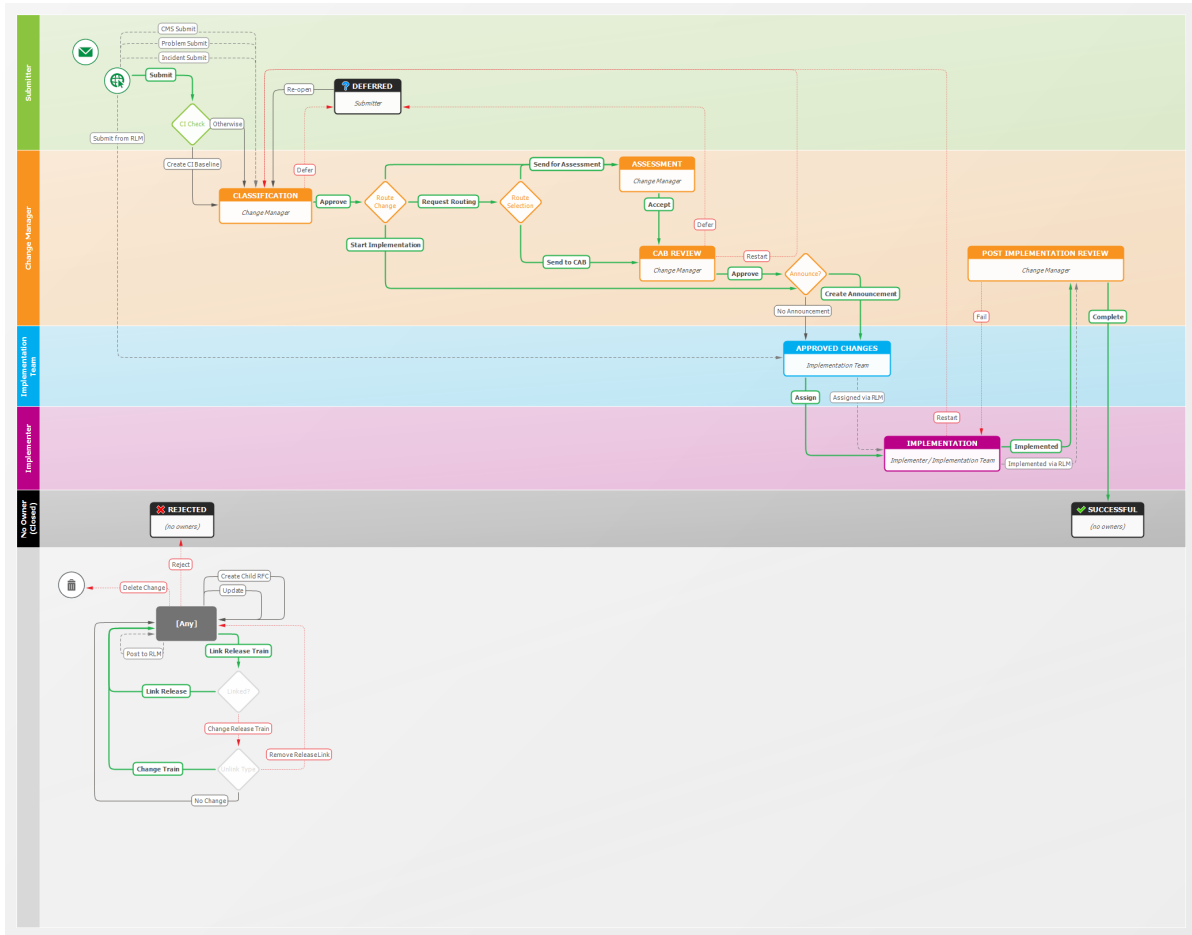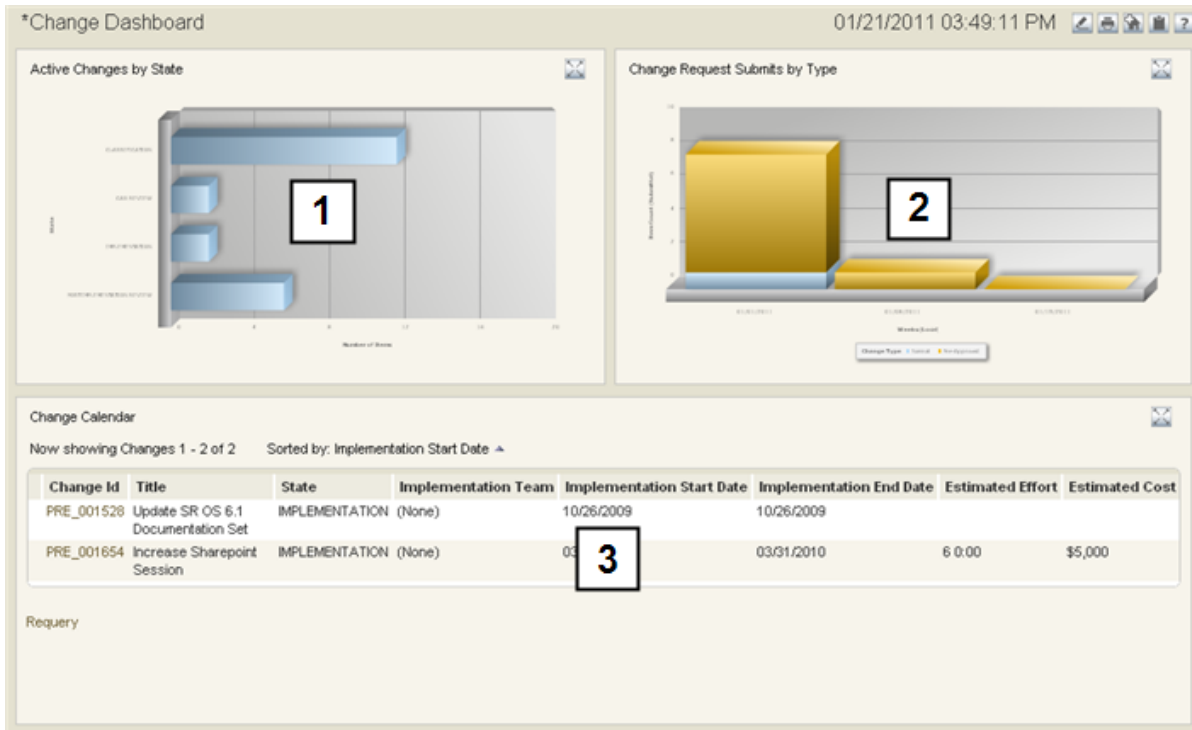
Change Management Dashboard

The Change Management dashboard is designed to alert change management staff to emergency RFCs and how long other RFCs have been active.

The **Change Dashboard** report is available in the reports that are shipped with the Change Management snapshot.

Tip: Set the Change Dashboard report as the home page report for the Change Management application by opening the **Changes** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.

1. **Active Changes by State** displays the number of changes in each state.

2. **Change Request Submit by Types** breaks down by type how many changes are submitted over the past few weeks.

3. **Change Calendar** shows the scheduled changes and when the changes are scheduled for.

> **Note:** The dashboard report is a multi-view report titled **Change Dashboard**. You can modify this report to add additional reports that help you to improve your Change Management process. You can modify the report under the Report pane in the SBM User Workspace.

Risk Dashboard

The Risk dashboard is designed to alert change management staff to the risk of upcoming RFCs. The reports on the dashboard make use of the Risk Analysis survey and the Risk Calculator to determine the risk of the changes.

The **Risk Dashboard** report is available in the reports that are shipped with the Change Management snapshot.

> **Tip:** Set the Risk Dashboard report as the home page report for the Change Management application by opening the **Changes** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.
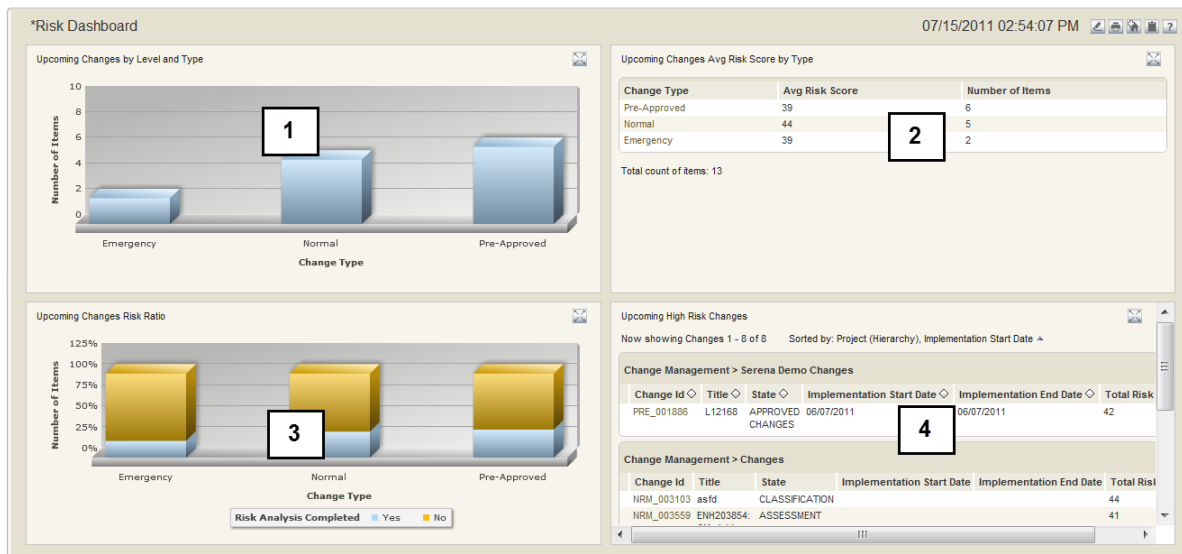
1. **Upcoming Changes** displays the number of upcoming changes broken down by change type. These changes have a completed Risk Analysis survey.

2. **Upcoming Changes Avg Risk Score by Type** breaks down the average risk score for the upcoming changes based on change type.

3. **Upcoming Changes Risk Ratio** shows the upcoming changes which have a completed Risk Analysis survey compared to the changes that do not have a completed survey.

4. **Upcoming High Risk Changes** has a list of upcoming changes with a risk score greater than 39. The items are sorted based on implementation start dates.

> **Note:** The dashboard report is a multi-view report titled **Risk Dashboard**. You can modify this report to add additional reports that help you to improve your Change Management process. You can modify the report under the Report pane in the SBM User Workspace.

Change Management Roles

The following roles (or actors) are available in the Change Management process app. Use the SBM Application Administrator to assign users to roles.

Change Manager - The Change Manager is responsible for the Change Management process, making sure that standard procedures for change are followed. Other duties include:

- Ensure efficiency and effectiveness of the Change Management process

- Manage Change Management staff

- Provide for continuous service improvement for Change Management

- Schedule regular configuration item verification and audits

- Produce KPI reports for management review

- Manage Forward Schedule of Change conflicts

- Conduct the Change Approval Board meetings on a regular basis

- Maintain the Change Management system

- Collaborate with other ITSM processes such as Problem Management, Issue Management, and Configuration Management

Change Implementer - This role is for change management staff who are responsible for implementing the change. The responsibilities of this role include:

- Own requests from implementation to closure

- Ensure that prior approval has been granted before executing the change

- Collaborate with requesters with the goal of implementing the requested change

- Inform change management staff of request status and resolution

- Coordinate with release management to ensure that processes are followed

- Provide Post Implementation feedback during PIR (Post Implementation Review)

Change Requester - This role is for the end users who will be submitting RFCs, providing the necessary details to the change implementers.

Change Administrator - This role is responsible for administering Change Management, such as assigning users to roles or fixing SBM issues.

Integration to Serena Release Manager

Note: This topic describes the components of Change Management which are designed for use with Serena® Release Manager (SRM). It only describes the pieces within Change Management and not the detailed explanation of how to use SRM with Service Manager. For detailed information on using the integration, refer to the Serena Release Manager documentation.

The Change Management process app has integration points with Serena Release Manager, which allow you to link an approved change request in SSM to a release train in SRM.

The integration appears in Change Management after a change has been approved and the request is in the **Approved Changes** state. A user can link a request to a release train by selecting the **Link Release Train** action.

Once a request has been linked to a release train, the request remains in the approved state until automatically transitioned by SRM. The **Update** transition will be the only available transition from the User Workspace, and the following message appears on the view form of the request: *This CR is linked to a Release Train and will be transitioned automatically by the Release Runbook. For more information please see the Release Train tab.* The **Release Train** tab on the view form will contain information about the release train.

Release trains can be added or changed for a request in the **Approved Changes** state by selecting the **Link Release Train** under **More Actions**.

Restriction: The **Link Release Train** transition is only available if Serena Release Manager is installed and the user has the required privileges to perform the link operation.

The **Link Release Train** transition routes the item based on whether the request currently is linked to a release train or not:

- If not currently linked to a release train, the **Link Release** transition path is followed. It uses the **Plan into Release Train** form, where the user can search for release trains on the **Planned Release** tab. The tab also contains two reports, which allow you to view current release trains. The reports are:

  - **All Planned Release Trains** (which shows all release trains that have been planned and are able to have items linked to them)

  - **Suitable Release Trains** (which filters the list of planned release trains based on the implementation dates of the change request and start date of the release train)

- If currently linked to a release train, the **Change Release Train** transition path is followed. It uses the **Update/Delete Release Train** form which allows the user to either change the release train or to unlink the current release train. The options to unlink or change the release train are found on the **Linked Release** tab. Choosing **Yes** will delete the current link. Choosing **Change** allows you to select a new release train.

After you have chosen a new release train for the item, the new information will be added into SRM.

Note: There is one additional SRM form that is included in Change Management, **Plan into Release Train Submit**. This form is invoked from SRM when submitting a new change request.

Chapter 9: Configuration Management System

The Configuration Management System (CMS) process oversees the lifecycle of the Configuration Items (CIs) through the fundamental elements of identification, status accounting, and audits. From initial activation to final deactivation, the CMS process enables you to track your IT Assets.

This CMS solution contains the **CI Relationships** application, which is used to store relationship information between your CIs. This information allows you to see how items relate to each other, and how dependencies among items affect your IT services.

- Configuration Management Overview [page 93]

- CMS Workflow [page 101]

- CMS Dashboard [page 101]

- CMS Roles [page 102]

Key Benefits

- Configuration Management Database with CI categorization according to ITIL.

- Management of complete Configuration Item lifecycle.

- Ability to create relationships between CIs and view relationships in a graphical format.

- Links between CIs and other items (such as Incidents, Problems, or Changes) enable quick problem diagnosis and change control of assets.

Configuration Management Overview

The configuration management application contains the following areas:

1. Configuration Identification [page 93]

2. Configuration Control [page 97]

3. Audit and Verification [page 99]

4. Status Accounting [page 99]

1. Configuration Identification

Creating and identifying Configuration Items (CIs) is the process in which new items are defined and added to the Configuration Management Database. Once an item has been added, it can be tracked and managed through its workflow. This enables you to perform the necessary audits using the reporting capability found in SBM.

New items can be created either automatically based on an event raised from another tool or manually from within SBM. Other tools that can be configured to raise events include

other Asset Management Systems or Asset Discovery Systems. New items may need to be created from within SBM based on a Request for Change (RFC), Service Request for new hardware, or the results of an Audit where items were discovered not to exist in the system.

> **Note:** Raising and receiving events within SBM requires knowledge of Web services and SBM orchestrations. If you do not have in-house expertise, contact Serena Professional Services, who can help you modify your Service Manager implementation to communicate with third party tools.

When you create or classify a CI, some fields have predefined values, such as the Category and CI Type fields. The predefined values enable you to select the appropriate entry for the item. The defined values create consistency among your configuration items, which in turn helps when searching for existing configuration items to relate to an incident or problem. In addition, the defined information improves the audit and report results for managing your configuration items.

The defined values are available from the drop-down lists on the Submit form. In the default Service Manager, values can be defined for CI types, Status, Categories, Sub-Category, Sub-Category Type, and Manufacturers. Note that the Sub-Category and Sub-Category Type include relational fields, which means that you must select a value in the related field before they will populate with values. For example, you must select a Category before values will appear in the Sub-Category field. And when you select a sub-category, the Sub-Category Type drop-down list will be populated.

> **Tip:** Some selection lists are populated from auxiliary tables, such as Category, Sub-Category, and Manufacturers. If you have permission to edit the table, you can add or modify selections by selecting ⬚, navigating to the auxiliary table (**Search | Manage Data**). or using an Editable Grid report run against the auxiliary table.
>
> Other lists are defined in the process app using SBM Composer. Updating these values requires that you redeploy the process app.

Some of the fields in CI items are free-form text fields, which allow flexibility when defining items. Examples of these fields are CI Name, Description, Maintenance Window, and Serial Number.

Your configuration management solution is customizable so that you can add fields to specify additional data, such as a date field of when the warranty expires. Custom fields can be added to the process app within SBM Composer and then deployed to your server.

After you complete the submit process by clicking **OK** on the submit form, the CI is created. It is assigned a unique identification number and it moves to the Classification state, where it is assigned to a Configuration Analyst. The analyst can choose how to proceed with the item. The analyst could choose to modify the CI by selecting to **Update** the item, and then choosing appropriate values for the item. If the analyst feels the CI is ready to activate or publish, the analyst clicks **Activate**. The configuration item is now live in the system, and it resides in the **Active** state in SBM until it is audited, inactivated, or disposed.

> **Note:** Functional and access privileges to configuration items are role-based and your role is defined by your administrator. Depending on your privileges, you may not be able to create new items, update items, or add relationships to items. Field attributes may also be classified, and access to each data classification can be granted according to your role. The right to transition changes from one state to another can also be controlled by the role privileges.

About Relationships

Service Manager stores not only your configuration items, but the relationships between the configuration items as well. Knowing these relationships helps you understand what may happen when an asset is modified. For example, your company's internal Wiki may be *hosted on* server A. If a change occurs to Server A, it can affect the internal Wiki.

In addition, relationships can be used to group CIs together under one main CI. For example, an IT service such as the ERP application can be defined as a CI, which is made up of an application, database, server, and network components to provide that IT service.

Relationships between active Configuration Items are displayed using the Relationship Explorer. The Relationship Explorer graphically depicts the relationships between the currently displayed item and other items. You can view the related items by selecting them from the graph. The Relationship Explorer displays on the **Relationships** tab for an active configuration item, and on the **CI Relationships** tab for the Incident, Problem, and Change processes.

> **Note:** The arrow in the Relationship Explorer points from the Primary CI to the Related CI. The Primary CI is the item that was specified as the Primary CI when creating the relationship. By default, the item which you are creating the relationship from is populated as the Primary CI.

> **Important:** When a new version of CI replaces an existing CI, the relationships are automatically transferred to the new version of the item.

Adding a Relationship

To add a relationship to a CI:

1. Open the active CI.

2. Select the **Relationships** tab and click **Add New Relationship**.

3. A Submit form displays to the Relationships auxiliary table. The current CI is automatically chosen as the Primary CI.

4. Select the **Relationship Type** and the **Related CI**.

5. Click **OK** to submit the form.

6. After the relationship is added, it will appear on the **Relationships** tab of the item. The **Relationships** tab shows all CI relationships to or from the active CI.

   > **Note:** Configuration item relationships are stored in the **Relationships** auxiliary table of the CMS process app.

Removing or Modifying Relationship

To remove or modify a relationship from a CI:

1. Open the active CI.

2. Select the **Relationships** tab.

3. Expand the **Relationship Maintenance** section. This section displays the primary relationships associated with the item.

4. On the report results, select the relationship to modify or delete. The relationship appears in a new tab.

5. Select from the available options to **Update** or **Delete** the relationship.

Navigating Relationships

The Relationship Explorer displays the relationships to the CI in a tree format. The main CI appears with a red border and is *centered* in the Relationship Explorer. By default, one level of relationship upward from the centered item is displayed, and up to five relationships downward.

Choose from the following actions on the graph:

- Display the details of an item in the graph by clicking on the title of the item.

- Focus the graph on another item by clicking the title bar of that item. This centers the graph on that item. You can recenter to the original CI by clicking **Restore**.

- Change the layout of the graph by choosing either **left to right** or **top to bottom** from the drop-down list.

- Zoom in by clicking **Full Size**. See the entire set of connections by clicking **Full View**.

  Tip: Vary the zoom level using your mouse wheel.

Adding a New Relationship Type

You can add, modify, and delete relationship types. The available relationship types are contained in the **Relationship Types** auxiliary table of the CMS process app.

To access the relationships:

1. Open the **Relationship Types** auxiliary table by running a report against it or by selecting **Search | Manage Data**.

2. Choose to modify, delete, or add a relationship type.

Creating CIs from Events

When the Service Manager adapter issues an event, the event triggers the creation of a configuration item.

The submission from the connector is populated with specific information that allows the new CI to be automatically routed to the **Active** state, by passing the **Classification** state.
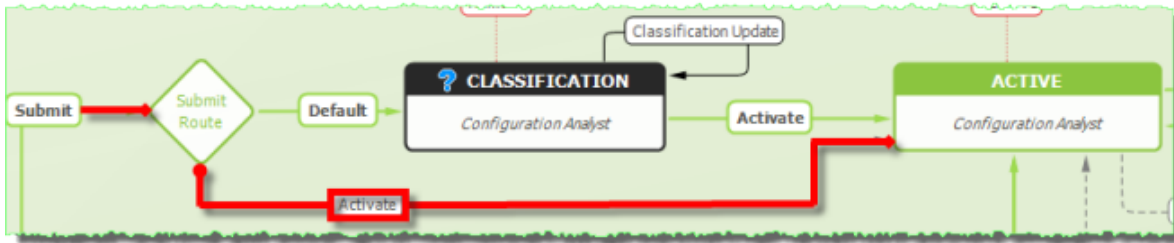
Note: Any submission that has these keys populated is auto-routed to the active state. Items manually submitted go to the **Classification** state.

2. Configuration Control

Service Manager configuration management has a set of processes and approvals that are required to change a configuration item's attributes. ITIL best-practice recommends that changes to CIs require an RFC. The default Service Manager configuration enforces the need of an RFC for certain changes to the CI. The RFC captures the details of the change, and it is managed by the Changes workflow, which enforces the collection of appropriate approvals and tracks the implementation steps.

The management of configuration items (CIs) may span across other process teams in addition to the configuration management team. For example, before a request for change is implemented, the attributes of the associated CI may need to be validated against the RFC by the change management team. And then after the change is implemented, the validation may be done again by the configuration management team to ensure consistency.

After the RFC has been approved and the changes made, SBM automatically baselines the existing CI and records the changed information. See Understanding Baselines [page 98] for more information on how baselines work in Service Manager.

Note: Updating from an RFC is different from using the **Update** transition on the item directly. The **Update** transition prevents modification of some fields such as version number. These fields can only be modified using an RFC.

The ability to create, manage, and update CIs and their attributes depends on how administrators assign roles within configuration management. Access privileges may grant read-only access for some roles, but update privileges for other groups. Data attributes can also be classified, and access to each data classification can be granted via the role. The right to transition changes from one state to another can also be controlled by the role privileges. Details of the roles in Configuration Management are described in CMS Roles [page 102].

Administrators can manage the workflow of CIs by determining owners for each state. Administrators can set rules that determine who the owner will be based on the CI attributes, which automates the workflow by automatically assigning items to the correct owner.

The fields that contain the CI attributes can be configured to be required or optional. You can fine-tune the requirements by marking the field as mandatory throughout the life-cycle of a configuration item (CI) or only for certain transitions from one state to another. Field settings are customized using SBM Composer.

Understanding Baselines

Baselines identify the significant states within the revision history of a configuration item. They capture the changes that were approved and implemented for a particular version of an item. By comparing the active item with its previous baselines, you can view the modifications that occurred between CI versions.

Service Manager uses separate items in the CMS workflow to track active CIs and baselines. The state of the item in CMS workflow determines whether the item is an active CI, an active baseline, or an inactive baseline. Links exist between baselines and active CIs, which allows Service Manager to track the baselines associated with each active CI.

The complete process for creating a new active CI and baseline using an RFC is as follows:

1. RFCs are required for a change to a CI. When you submit an RFC against an active CI, a new CI is also submitted. The new CI is placed in the **Pending Change** state, where it remains until the change is completed. The new item is linked to the active or original CI, and it is pre-populated with information from the existing CI. You can find a link to active CI from the new CI on the **Config Item** tab. You will see the version number has been incremented automatically on the new CI.

2. The original CI moves to the **Baseline Pending** state, informing you that a new CI is in process of being implemented.

3. After the RFC is closed, the new CI moves to the **Verification Required** state, where the change is verified by the Configuration Analyst to ensure that it matches what was expected.

4. After being verified, the new CI becomes the active CI. The original CI transitions from the **Pending Change** state to the **Active Baselines** state, marking it as a baseline.

5. You can see related active baselines for a CI by displaying the report on the **Baselines** tab.

6. A baseline can replace the active CI by selecting to **Restore** it. This creates an RFC and a duplicate of the baseline item. After the RFC is completed, the duplicate item will become the new Active CI.

In summary, an item in the CMS workflow can have the following possible designations as it moves through the workflow:

- An **Active CI** is the current version of the CI.

- A **Pending Change** is an item that is waiting for an RFC to be complete before it becomes the active CI.

- An **Active Baseline** is a non-current version of the CI. It resides in the **Active Baselines** state. You can see the active CI on the **Config Item** tab. An Active baseline does not display the other baselines on the **Baselines** tab. The report will be empty.

- An **Inactive Baseline** is a version of the CI that has been deactivated. Deactivated baselines do not appear in the Baselines report that appears on the **Baselines** tab. You can find inactive baselines by running a report against the CMS project which contains the baseline items. Remember to include inactive items in your report.

Keep in mind the following when working with baselines:

- All opened RFCs must be closed before the CI will transition to the next state. That is, if you have multiple RFCs opened up for one CI, all of these issues must be closed before the CI becomes the new active CI.

3. Audit and Verification

Audit and verification checks for the existence and accuracy of information contained in the CMDB against the actual asset. If any exceptions are realized, then the CMDB has to be updated appropriately.

In Service Manager, a configuration analyst can choose to audit an item by selecting the **Audit** transition and adding any applicable Work Notes. The CI moves to the Audit state, where the CI is verified. If a discrepancy is found or a change is required, the configuration analyst can choose from a variety of transitions to determine what happens to the CI:

- **Verify** – To mark the CI as verified against the actual asset, returning the CI to the Active state.

- **Not Found** – To mark an item as not found.

- **RFC Posted** – To raise a Request for Change to fix an issue or exception found during the audit.

- **Dispose** – To mark an item as disposed.

- **Inactivate** – To mark an item as inactive.

> **Note:** Service Manager supports the process of auditing and verification, but the actual act of auditing or verifying a configuration item has to be performed by a member of the configuration management team.

Configuration items, their versions, and their changes form the basis of any configuration audit, and SBM enables you to create and run reports on these items. Service Manager comes with some default reports, and users can create additional reports by selecting **Create Reports** in the **Reports** pane of the SBM User Workspace.

Some of the out-of-the-box reports include:

- Configuration Items by State

- Configuration Items by Type

- Missing Configuration Items

- All Laptops

- All Servers

4. Status Accounting

Status accounting for configuration items (CIs) refers to the ability to record and report on the status of all CIs that are under control of the Configuration Management System (CMS).

Any activity performed on the CI from creation to disposal is recorded, providing an audit trail throughout the CI lifecycle. Records are marked with the activity date and ID of the individual who performed the action. This means that you can see when and who updated items, performed transitions, or added relationships to a particular item.

Status information is used for successful configuration audits, where the configuration management team wants to see the current status of the CIs. For reporting by the service management team, Service Manager comes with many out-of-the-box reports that are used to find the status of your CIs. In addition, you can easily create custom reports to display information that you require.

Status information may also be needed by other service management processes, such as Change Management and Problem Management, to relate new RFCs, problems, and workarounds to particular configuration items. Other Service Manager processes link directly to the configuration management application, enabling you to find CI information from within the context of the other process. For example, the incident management, problem management, and change management processes require that you choose a CI to relate to the new issue, and this can be performed directly from the form using the relational field search box.

SBM reports are important for keeping up-to-date on your configuration status. Status reports should be produced on a regular basis and include:

- Lists of all CIs under control, their current version, and change history

- Status accounting reports on the current, previous, and planned states

- Unique identifiers of constituent CIs and their current status

- Configuration baselines, releases, and their status

- Latest software item versions and their status for a system baseline

- Persons responsible for making status changes

- Change history and audit trail

- Open Problems and RFCs.

Status accounting reports can be used to establish system baselines and enable Changes between baselines and Releases to be traceable. Status reports may include:

- Baseline and release identifiers

- Latest software item versions for a system builds

- The number of changes for a system

- The number of baselines and releases

- The usage and volatility of CIs

- Comparisons of baselines and releases.

In addition to reports, notifications can be used to keep informed about CIs. SBM enables users to subscribe to notifications for changes to CI, such as a state transition or an update. Service Manager comes with default notifications. Additional notifications can be created and configured using SBM System Administrator. For example, you may be

responsible for your production servers, and you want to be notified whenever a CI item related to servers is updated. Your administrator can create a notification that looks for certain conditions, such as updates on items related to production servers, and then sends an e-mail notification when the event occurs. An end user can subscribe to any notification to which they have access by configuring the notifications under their **User Profile** in the SBM User Workspace.

CMS Workflow

The Configuration Management System workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Active* and *Audit*, and the transitions are marked with arrows, such as *Close* and *Activate*.

The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM Application Administrator. Use SBM Composer to modify the workflow.
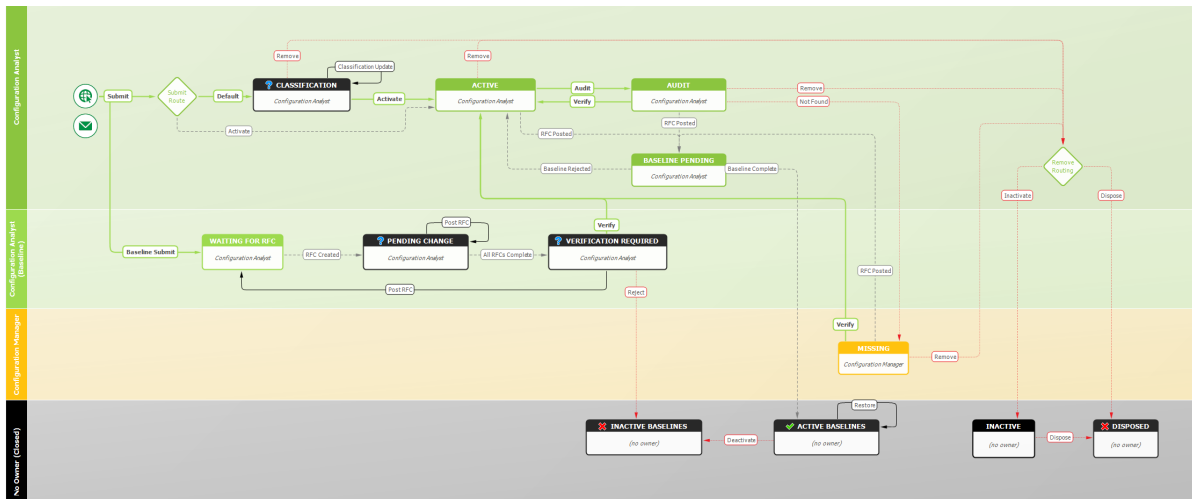

CMS Dashboard

The CMS dashboard gives an overview of your existing assets, incidents associated with those assets, and ongoing requests for change.

The **CMS Dashboard** report is available in the reports that are shipped with the Configuration Management System snapshot.

> **Tip:** Set the CMS Dashboard report as the home page report for the CMS application by opening the **CMS** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.
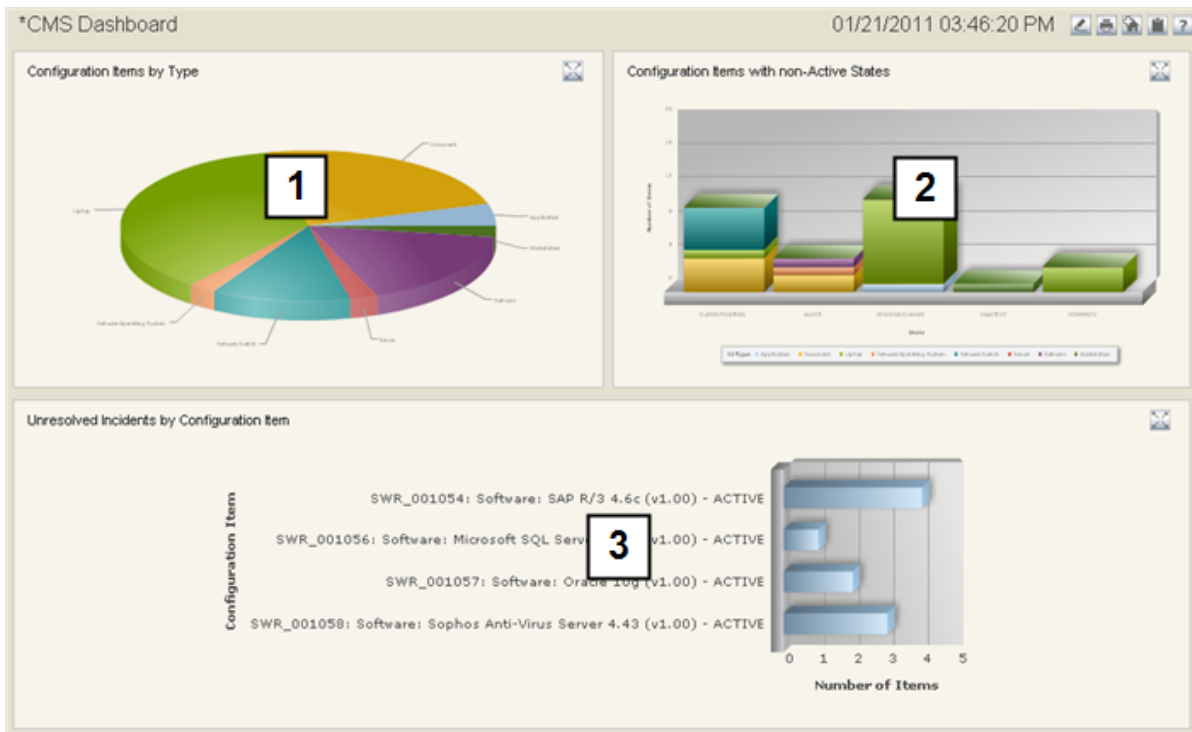
1. **CI by Type** gives an overview of the distribution of assets that you have across your company.

2. **Configuration Items with Non-Active States** shows a breakdown of where CIs reside when they are not active.

3. **Unresolved Incidents by Configuration Item** shows the open active incidents broken down by CI asset. This gives you a high-level perspective of how many incidents are being raised against each CI item, enabling you to see problem areas which should be investigated or changed.

CMS Roles

The following roles (or actors) are available in the Configuration Management System process app. Use the SBM Application Administrator to assign users to roles.

Configuration Manager - The Configuration Manager is responsible for the Configuration Management System and the CI Relationships. Other duties include:

*   Ensure efficiency and effectiveness of the Configuration Management process

*   Define Configuration management policy including scope

*   Promote continuous service improvement for Configuration Management

*   Produce KPI reports for management review

*   Schedule regular Configuration Item verification and audits

*   Maintain the Configuration Management system

- Monitor the quality of the CI records and their usefulness to the other Service Manager processes, especially identity management, problem management, change management, and release management

- Monitor the quality of CI information including CI-to-CI relationships

- Develop methods and procedures for populating the CMDB

Configuration Analyst - This role is for configuration staff who are responsible for monitoring the CI records. The responsibilities of this role include:

- Coordinate Configuration management activities including CI identification, control, audit, and verification

- Collaborate with Change management on updating CI records

- Produce KPI reports

Configuration User - This role is for the end users who will be submitting new CIs or searching for CIs to relate to incidents, problems, or requests.

Chapter 10: Knowledge Management

Serena Service Manager has a new and improved Knowledge Center, for managing knowledge base articles and announcements. The Knowledge Management application allows you to manage the submission of new articles and to monitor changes to existing articles.

The Knowledge Management application has two main types of users:

- *Contributors* are responsible for submitting articles and adding content. They edit the content of the articles, adding formatting to text, such as italics and bulleted lists, using the embedded HTML widget. The contributors are able to save the articles as drafts, which stores the data in the database until the article is ready to be sent to the publisher for final approval.

- *Publishers* review articles before they are made available to end users. The publisher can send the article to additional team members for approval. When the article is ready, the publisher is responsible for posting or publishing the articles to Knowledge Center.

Once it is published, the Knowledge Management item is closed and the content is copied to the Knowledge Center where the material becomes available to end users. **Urgent** announcements are displayed to the user in the banner bar of Request Center.

The article now resides in Knowledge Center. Users can comment and rate the article, and these comments and ratings are stored in Knowledge Center.

The content of the published articles cannot be edited directly in Knowledge Center. Instead, a new item is submitted into Knowledge Management using the **Update this item** link on the published article. The new item must proceed through the same Knowledge Management workflow. When the change is published, the updated content replaces the existing content in Knowledge Center, while the comments and ratings will remain unchanged.

The following topics describe the features found in Knowledge Management:

- Knowledge Management Roles [page 106]

- Working with Articles from the User Workspace [page 106]

- Working with Articles from Request Center [page 112]

- Knowledge Management Workflow [page 114]

- Knowledge Management Dashboard [page 115]

Key Benefits

- HTML Editor for easy formatting of article content.

- Four distinct types of articles to distinguish types of information within Knowledge Center.

- Distinct user roles for publishers and contributors to ensure quality of Knowledge Center content.

- Tracking of approvals to ensure knowledge base article quality.

Knowledge Management Roles

Tip: After adding users to the roles described below, set default values for the Publisher and Contributor fields at the project level. The default values prevent possible permission errors which can result when Knowledge Management articles are submitted from other process apps.

The following roles are available in the Knowledge Management process app. Use the SBM Application Administrator to assign users to roles.

Note: Members in all of these roles are available for selection when an item is sent for approval.

Editor/Publisher - The Publisher is responsible for editing, approving, and publishing Knowledge Center articles.

- Submit new articles to add to Knowledge Center

- Start the update process by submitting items for existing Knowledge Center articles

- Approve articles before they are published, ensuring that Knowledge Center articles meet the accepted standards

Contributors - The Article Writer is responsible for adding content to Knowledge Center articles. Other duties include:

- Add content to articles that are in the **Edit** state.

- Edit existing knowledge base articles that have been re-opened

- Review and approve content of an article written by another contributor

Announcement Contributors - The Announcement Contributor has the same privileges as the Contributor. In addition, the Announcement Contributor has the ability to publish announcements without requiring Publisher approval.

KM Administrator - This role is responsible for administering Knowledge Management, such as assigning users to roles, fixing SBM issues, or restoring deleted items.

Working with Articles from the User Workspace

The following topics explain the Knowledge Management activities performed in the User Workspace:

Creating Announcements and Articles

Knowledge Center articles and announcements can either be created directly by submitting a new item into Knowledge Management or by spawning an article from an incident, request, problem, or RFC. Both of these actions occur from with the User Workspace.

Articles are submitted into the Knowledge Management workflow. The articles are originally assigned to contributors, who add content to the article. Contributors may save the articles as drafts, allowing them to work on the items at a later time.

Contributors can make two types of modifications to the articles: changes to the metadata and changes to the content. The metadata includes expiration dates, summary, and keywords, and this data appears on the **Overview** tab of an article. The **Content** tab is where you modify the actual contents of the article.

Overview Tab

The following sections describe settings that you can make on the **Overview** tab.

Article Types

Knowledge Management articles are divided into four types, with some of the types being associated with a particular items. The four types with their respective items in parentheses are:

- **Announcement** (Changes)

- **FAQ**

- **How To**

- **Tech Note** (Incidents, Requests, Tech Notes)

Announcements that are marked as **Urgent** appear both in Knowledge Center and in the announcement bar below the banner of Request Center.

Urgent Announcements

Check the **Urgent** option to mark an announcement as urgent, meaning that the announcement will be displayed prominently below the banner of the Request Center. Urgent announcements will still appear in search results on the Knowledge tab.

Users can navigate through the urgent announcements in the announcement bar by using the up and down arrows.

The following arrow shows an example of an **Urgent** announcement in Request Center.
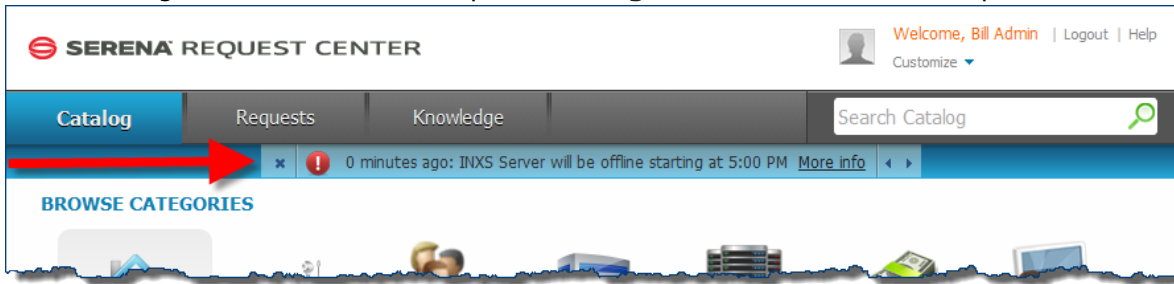
Note: The IT administrator may disable the announcement bar in the Request Center.

Categories

Knowledge Center users can filter articles based on categories, allowing them an easier way to find knowledge base articles. A Knowledge Management article can be assigned to a particular category when it is created or modified.

To add, modify, or delete categories, access the **KM Categories** auxiliary table by selecting **Search | Manage Data | KM Categories** in the User Workspace.

You can choose an image to represent each category by clicking **Change image**. For information on the image picker, see About the Image Picker [page 39].

Restriction: Modifying items in the **KM Categories** auxiliary table requires the appropriate permissions.

Article Duration

Define how long the article will be available to end users in Knowledge Center by selecting the **Article Duration**. **Does not expire** means that you select when the article becomes active in Knowledge Center and the article will not be removed automatically at a specific date. **Expires** allows you define both the **Start Date** and **Expiration Date** for when the article will be available in Knowledge Center.

For example, you may be performing maintenance on your e-mail server this weekend, and you want to inform your users that the services will be off-line from noon to midnight on Saturday. You would set expiration date and time at the end of the Saturday. The announcement will no longer appear in Knowledge Center after the expiration date.

Users who have the privilege to **Submit** articles can view expired articles by selecting **Include Expired** articles in Request Center.

Keywords

When a user performs a Knowledge search in Request Center, the search is performed against the keywords defined for each article. The **Keywords** are automatically generated when an article's content is updated. The keywords for the article are displayed in the read-only **Keywords** field.

The keywords are also used for the item match search that is performed when a user submits an item.

Tip: The **Summary** field is not included when generating the keywords. Remember to include searchable terms from the **Summary** in the **Content**.

See the following section for information on how the keywords are generated.

About Keyword Generator

The keywords are generated using a script called wordStats. It generates the 35 top keywords for the document. The top keywords are found by stripping out the stop words (see following list) and then applying a weight to the words based on their frequency and on the style in which the words reside.

See the following sections for information on the weight for each style and the list of stop words.

For more information on wordStats, see: http://hovinne.com/articles/jquery-wordstats-plugin

Weighting

When a word is found in a particular style, it is assigned the following weight. If the word is found multiple times, the weights of the various instances are summed.

Style	Weight
Title	20
Heading 1	15
Heading 2	10
Heading 3, Heading 4, Heading 5, Heading 6	5
B, I	3
Paragraph, Lists, Links	2
Image Title	1

Stop Words

The keyword generator skips all one letter words. In addition, the following words are ignored:

about, after, ago, all, also, an, and, any, are, as, at, be, been, before, both, but, by, can, did, do, does, done, edit, even, every, for, from, had, has, have, he, here, him, his, however, if, in, into, is, it, its, less, many, may, more, most, much, my, no, not, often, quote, of, on, one, only, or, other, our, out, re, says, she, should, so, some, soon, such, than, that, the, their, them, then, there, these, they, this, those, though, through, to, under, use, using, ve, was, we, were, what, where, when, whether, which, while, who, whom, with, within, you, your

> **Note:** An apostrophe is considered a word break, which means that abbreviations are treated as two words. For example, *you've* is considered to be *you* and *ve*.

Content Tab

The content of the article is shown on the **Content** tab. The text is divided up based on sections.

> **Note:**
>
> When submitting a new article, the **Content** tab includes the ability to select an Article Type and to choose to **Load Article Template** associated with that article type. The article template includes sample data and headings to assist in completing the different sections according to company standards.
>
> After an article is submitted, the ability to load an article template is no longer available and the **Article Type** drop-down moves to the **Overview** tab.
>
> For more information on the article types, see Article Types [page 107].

Add content to the different sections by placing your cursor in the section and adding the text. When editing text in non-title fields, the HTML editor appears, which allows you to apply formatting to the text and insert links or images. The following topic describes how to use the HTML editor.

> **Note:** You cannot add images to the article on the submit form. You must complete the submit form by selecting **Save as Draft** and clicking **OK**. This completes the submit process and creates the item. Then, you select **Edit** and add the image to the content.

Using the HTML Editor

The HTML Editor allows you to format the text that appears within your articles and announcements. The editor allows you to apply heading formats, add bulleted lists, format text, and insert images or links.

The HTML Editor appears on the **Content** tab of the Submit and Edit transition forms in Knowledge Management.

To use the HTML editor:

1. Select the text to modify or place your cursor in the section to add the text. The HTML Editor displays the following menu:

2. Format a section by selecting it and then selecting the formatting, such as **Bold** or **Heading 1**.

3. Insert an image by selecting the **Insert** tab and clicking . Select whether to reference a URL for the image or to upload the image as an attachment.

   Uploading the image as an attachment is a two-part process. First, you select the insert image button to upload the image. This launches the Attachment dialog, where you can browse to the image to upload. After the upload completes successfully, then select the insert button again, and choose the image in the drop-down menu.
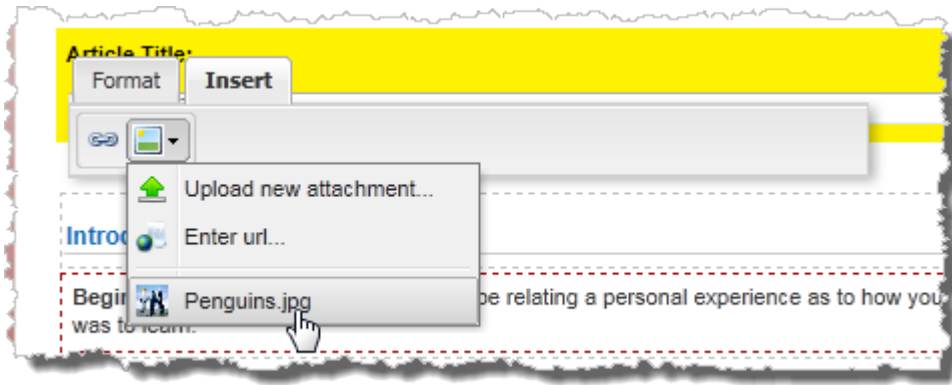
The image will now appear inline. In summary, the image file will be stored as an attachment in the item, and it appears inline in the content.

4. Make text a hyperlink by selecting text and clicking 🔗 . The **Link** tab opens. Enter the URL for the hyperlink. The hyperlink will become active after the page is saved.

   Note that if text is not selected, the text `New Link` will be added. This text can be modified to change the name of the link.

   You can modify an existing link by clicking on the link in Edit mode. This will open the **Link** dialog to edit the hyperlink. Click 🔗 to remove the link.

Displaying Labels

On the **Content** tab, labels appear on the right side which help to define what type of content each section should contain.

You can show or hide the labels by clicking **Show Labels** or **Hide Labels** link on the top of the tab

Reviewing Articles

Reviewing articles before they are published for public viewing in the Knowledge Center ensures that your articles meet the standards set by your company.

The main actors for reviewing articles are the editor/publisher and reviewer. The editor/publisher is responsible for sending the article for review, adding suggested edits to the article, and publishing the article. The reviewers who are responsible for reviewing the article and suggesting edits.

The complete steps for review process in Knowledge Management are as follows:

1. Contributor finishes an article and sends the article to the editor/publisher using the **Send to Publisher** transition. The article moves to the **Content Preparation** state.

2. The publisher chooses to send the article for review by selecting the **Send for Review** transition.

3. On the transition form, the publisher chooses the reviewers by moving them into the **Reviewers** list.

4. After adding the **Work Notes** to the article, the publisher completes the transition by clicking **OK**.

5. The article moves to the **Content Review** state, where the selected reviewers become the owners.

6. The reviewer can **Approve** the article or **Suggest Edits**. The suggested edits are noted in the **Suggested Edit** field.

7. When a reviewer suggests edits to the article, the article moves to the **Edits Suggested** state after the reviews are completed.

8. The publisher can choose to **Edit** the item and add the suggested edits.

9. After the edits have been incorporated, the publisher chooses to either publish the article or send the article for another round of review.

In addition to the usual review path, publishers can choose from the following options:

- **Return** the article to the contributor, which moves the article back the **Draft** state. The contributor can add to the article and then send it back to the publisher.

- **Reject** the article, which moves the article to the **Rejected** state. The contributor to the article can choose to **Re-Submit** it.

- **Cancel review** of the article, which returns the article to the publisher. If suggested edits have been added, the article moves to the **Suggest Edit** state. If not, the article returns to the **Content Preparation** state.

- **Delete** the article, removing it from the system.

Publishing Knowledge Center Articles

Publishing an article moves the article into Knowledge Center, where it becomes active, available for searching, rating, and commenting by users. Publishing articles copies the content from the article in the Knowledge Management application into the Knowledge Center.

Publishing occurs with the **Publish** transition. The Publish transition is available from multiple states within the Knowledge Management workflow.

> **Important:**
>
> Do not use Mass Update or the Editable Grid to perform the **Publish** transition.
>
> The article will not be published to Knowledge Center, and the item will move to the **Published** state in Knowledge Management preventing you from publishing the article again. You will have to recreate the article.

After the article is published, modifications require that a new item is submitted into Knowledge Management by clicking **Update this item**.

Working with Articles from Request Center

The following topics explain the Knowledge Management activities performed in Request Center:

- Viewing and Commenting on Articles [page 113]

- Updating Knowledge Center Articles [page 113]

- Deleting Knowledge Center Articles [page 114]

Viewing and Commenting on Articles

Knowledge Center articles can be viewed from the Knowledge tab in Request Center, the Knowledge Management dashboard report, and from Incident submission forms.

The detailed article view allows users to read the content of the article, comment on the article, and give the article a rating. The average rating of the article and the number of views the article has received is tracked for users to sort on highest rated and most popular articles.

The following sections include information on tasks to perform from the detailed view.

Adding Comments or Ratings

Each user is allowed one comment or rating, and can change the comment or rating at any time.

To add or update comments, the user must display the article, and then click **Add your own comment**.

Sending a Link to the Article

Send the article to another person by copying the URL and pasting it in an e-mail or IM.

To copy the URL to your clipboard, click . You can then paste (CTRL+V) the URL into an email or IM. This URL allows users direct access to the article.

Updating Knowledge Center Articles

You may need to modify the published articles in Knowledge Center to add information or to fix errors.

Modifying a published article requires that a new item is submitted into Knowledge Management in order to track the changes. The new item contains a copy of all the information contained in the published article. The published article remains in Knowledge Center.

This duplicate item proceeds through the same Knowledge Management workflow, requiring the approvals, if needed. When the item is published, the new content replaces the content of the existing article in Knowledge Center. The comments that were made against the original article remain in Knowledge Center.

> **Restriction:** To modify an existing article, you must have publish permissions.

> **Important:** Administrators must set a default value for the Contributor and Publisher fields at the project level to avoid errors when submitting or transitioning articles in Knowledge Management. One option is to set the default value of the Contributor field to the **Current User**, which will assign the item immediately to the submitter for editing.

To modify an existing article:

1. Select the Knowledge tab in Request Center.

2. Find the article to edit by performing a search.

> **Note:** Access expired articles by selecting **Include Expired**.

3. Open the article then click **Update This Article**. A new item is submitted into Knowledge Management with the **Content** is populated with the data from the original.

4. Edit the article using the Edit transition and the HTML editor.

5. After finishing the modifications, publish the article to replace the existing content in Knowledge Center.

Deleting Knowledge Center Articles

You may need to delete or remove articles that are in the Knowledge Center.

To remove items, you will perform an update of the item from Knowledge Center as described in Updating Knowledge Center Articles [page 113], and then you set the expiration date in the past. Remember that the start date must be prior to the end date or the article will be considered a non-expiring article.

This will remove the article from the Knowledge Center, while keeping an audit trail of the item, informing others about who was the one responsible for removing the article.

Other publishers will be able to view the deleted article and its contents by selecting to view expired articles in Knowledge Center.
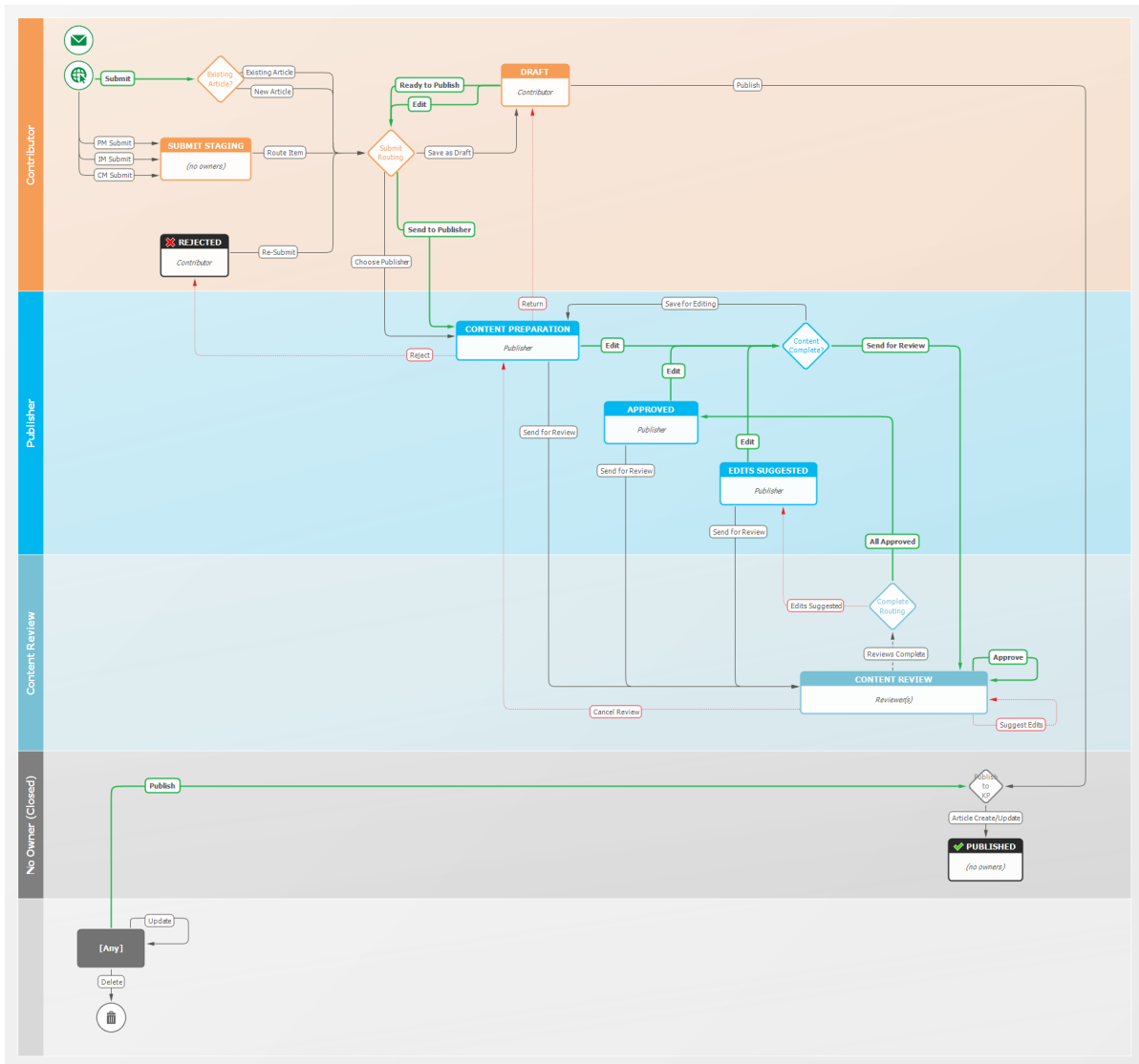
Knowledge Management Workflow

The Knowledge Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Deferred* and *CAB Review*, and the transitions are marked with arrows, such as *Reject* and *Accept*. The process starts with one of the different submit paths, and then it can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM Application Administrator. Use SBM Composer to modify the workflow.

> **Note:** When an article is submitted from another application, the option to **Send to Publisher** is disabled. The user must save as a draft before sending the article to be published. This eliminates problems that may occur if default values have not been set for the publisher or if the submitter does not have appropriate permissions.

Knowledge Management Dashboard

The Knowledge Management dashboard gives an overview of the existing knowledge base articles, trend lines of published articles, and articles currently in the process of being published.

The **Knowledge Management Dashboard** report is available in the reports that are shipped with the Knowledge Management snapshot.

> **Tip:** Set the Knowledge Management Dashboard report as the home page report for the Knowledge Management application by opening the **Knowledge Management** application in the User Workspace, clicking the **Application Settings** icon ( ), and choosing the report under **Home Page Report**.

1. The **Published Articles** widget displays the recently published articles in the same format that appears in Request Center. Choose from different display options such as filtering to display articles in one category.

2. **Published Article Trend by Type** shows the trend of how many articles are being published each week, based on the article types.

3. **Articles in Progress** shows the open active articles that have not been published and that are not in the draft state. Once articles are published, they are marked as inactive.

Chapter 11: Additional Information

This chapter has some additional information to understanding Serena Service Manager.

Adding Auxiliary Data

The Serena Service Manager makes use of data that is stored in auxiliary tables. These tables must be populated with some information in order to use the solution; however, the tables are meant to be added to as you add more information into your systems.

> **Important:** You must grant a user privileges to the tables below using SBM Application Administrator before you can populate them with auxiliary data in SBM Application Administrator.

CAUTION:

> The bold tables in these lists are populated by the solution. Use extreme caution when manually altering these tables.

The non-bold tables have default values but can also be tailored for your needs. The values determine which selections are available when working with incidents, problems, changes, and CIs. See Managing Auxiliary Data [page 119] for information on how to add information to these tables.

Serena Request Center Process Apps and Auxiliary Tables

The following auxiliary tables are packaged with the **Serena Starter Pack 3.0** process app:

- **KP Published**

- **KP UserRatings**

The following auxiliary tables are packaged with the **Knowledge Management** process app:

- KM Categories (Knowledge Management)

The following auxiliary tables are packaged with the **Service Desk** process app:

- Client Software

- Computer Models

- Computer Types

- Departments

- Mobile Carriers

- Mobile Device Platforms

- Mobile Devices

- Operating Systems

- Resolution Codes

- Symptom Codes

Serena Service Manager 3.0 Process Apps and Auxiliary Tables

The following auxiliary tables are packaged with the **Change Management** process app:

- None

The following auxiliary tables are packaged with the **Configuration Management System** process app:

- CI Categories

- CI Sub-Categories

- CI Sub-Category Types

- Model Numbers

- Relationship Types

- **Relationships**

- Software Platforms

- Vendors

The following auxiliary tables are packaged with the **Service Desk** process app:

- Client Software

- Computer Models

- Computer Types

- Departments

- Mobile Carriers

- Mobile Device Platforms

- Mobile Devices

- Operating Systems

- Resolution Codes

- Symptom Codes

The following auxiliary tables are packaged with the **Problem Management** process app:

- **Workarounds**

Managing Auxiliary Data

To add or edit data records to your auxiliary tables, choose one of the following:

- Log in to SBM Application Administrator as a privileged user, select **Auxiliary Data**, choose the table from the drop-down list, and then click **New** or search for an existing item to edit. For details, refer to the *SBM Application Administrator Guide*.

- Log in to SBM User Workspace and create an Editable Grid listing report based on the auxiliary table, and then either create or edit items in the table. For details, refer to the *SBM User's Guide*.

Modifying Process Apps

SBM Composer is used to modify process apps, applications, and orchestrations. This includes designing states, transitions, forms, actions, and other elements. You also use SBM Composer to create new roles and tie the roles to particular states or transitions.

To modify the process apps using SBM Composer:

1. Open the process app in SBM Composer by clicking **Composer Button | Open | Application Repository** and selecting the process app.

2. Repeat for all Service Manager process apps. This allows reference information to be loaded into SBM Composer local cache.

   Important: Open all process apps in SBM Composer before attempting to edit. The apps reference each other, and if one is not imported into SBM Composer, you may get validation errors.

3. Open the process app to modify.

4. Modify the process app.

5. Deploy the changes to your server.

For more information on using SBM Composer, refer to *SBM Composer Guide*.

Managing Users

To simplify the management of your users, roles have been created for the different applications. Administrators assign users to the appropriate roles, which gives the users the appropriate permissions and access to the applications.

> **Note:** User and Multi-User field types refer to the roles for populating the lists. For example, the **Additional Contacts** field refers to all of the roles used in Incident Management.

Managing users is a twofold process:

1. Create a user account.

2. Using SBM Application Administrator, add the user account directly to a role or add the user to a group that is granted the role.

See the topics associated with each application for more information on the roles available in the application:

- Incident Management Roles [page 60]

- Request Fulfillment Roles [page 68]

- Change Management Roles [page 90]

- Problem Management Roles [page 77]

- CMS Roles [page 102]

- Knowledge Management Roles [page 106]

Enabling Notifications

Notifications keep users and staff aware of changes to items. These notifications are contained in the application snapshots that were promoted during installation.

After the snapshots have been promoted, the administrator must grant **allow subscription** privileges to the users who will subscribe to the notifications. Once a user has been allowed subscription to a notification, the user or the administrator can subscribe the user to a notification. The administrator grants these privileges using the SBM Application Administrator.

Users manage subscriptions on the **Notifications** tab of their User Profile. The users can subscribe or unsubscribe to notifications.

Service Manager contains specialized notifications and notification templates in addition to the default notifications usually available with SBM applications. The following notifications are the default ones available for a deployed process app.

- Any [item] changes owner

- Any [item] changes state

- Any [item] changes to inactive

- Any [item] I submitted changed state

- Any [item] I submitted changed to inactive

- Any [item] is submitted

- I become the owner of any [item]

The following table explains the additional or modified notifications available with each process app:

Application	Notification Name	Change to Rule
Incident Management	IM - Any Incident is Submitted	Notifies **Reported By** and **Affected By** user when incident is submitted.
Incident Management	IM - Automatic Escalation to L2	Notifies when change moved to **Investigation & Diagnosis** state.
Incident Management	IM - Resolved	Notifies **Reported By**, **Affected By**, and **Additional Contacts** users when incident is moved to **Resolved** state.
Incident Management	IM - Resolved Repeat Cancel	Notifies user when incident moves from **Resolved** state.
Incident Management	IM - Resolved with Workaround	Notifies **Reported By**, **Affected By**, and **Additional Contacts** users when incident is moved to **Resolved by Workaround** state.
Change Management	CM - Change Submitted	Notifies the submitter when a change has been submitted.
Change Management	CM - Change Closed	Notifies the submitter and the user selected as the contact when the change is closed.

Service Manager also contains specialized templates. For on-premise installations, these templates are prefixed by ITSM and are installed into the notification templates directory:

```
SBMinstallationDirectory\Serena\SBM\Application
Engine\emailtemplate\notificationtemplates
```

Integrations Between Applications

The following sections explain the different links between items.

Related CIs

Once a CI is related to an item in another process, the information from that CI can be found within the other management process. For example, once an item is assigned to a CI, any CIs related to that CI appear on the Relationships tab for the item. This allows other management teams to gather necessary CI status information, and to create reports to determine if any particular CI is related to multiple problems.

CI status is also used for workarounds, which are related to a particular CI. This allows users to find possible solutions to a problem based on the item which is causing the problems. They can also search for solutions based on the CIs that are related to the item giving them problems.

Relational Fields

All of the process apps have relational fields that point to other applications. For example, the Problem Management application has relational fields that point to the CMS and CI items. This allows you to relate Configuration Items with problems and select from the same CI Categories.

Post-Transitions

Many of the process applications use post-transitions to submit items into other applications.

For example, the Problem Management application contains the **Post RFC** transition, which creates a request in the Change Management application.

Storing File Attachments

Attachments to items may be stored in SBM or in Microsoft Office SharePoint, depending on what options you have enabled with SBM. Serena offers SBM Connect for SharePoint®, a connector to SBM which allows you leverage the file management capabilities of SharePoint with SBM. For more information about SBM Connect for SharePoint®, refer to *Integration Guide for SharePoint* or contact Serena support.

Additional ITIL References

The following sites contain additional information about ITIL standards.

- **OGC Official ITIL® Website**: http://www.itil-officialsite.com

- **Wikipedia Article on IT Service Management**: http://en.wikipedia.org/wiki/IT_Service_Management

- **itSMF International - The IT Service Management Forum**: http://www.itsmfi.org/