White Paper
November 2006

BMC® Best Practice Process Flows for Asset Management and ITIL Configuration Management

Restricted Rights Legend

Contacting Us

If you need technical support for this product, contact Customer Support by email at customer_support@bmc.com. If you have comments or suggestions about this documentation, contact Information Development by email at doc_feedback@bmc.com.

This edition applies to version 7.0 of the licensed program.

BMC Software, Inc.
www.bmc.com

Contents

Chapter

1 Introduction

This white paper describes the process flows implemented in the BMC® Remedy® 7.0 Asset Management application, and based on IT Infrastructure Library (ITIL) best practices for configuration management.

The BMC Remedy Asset Management application lets IT professionals track and manage enterprise configuration items (CIs)—and their changing relationships—throughout the entire asset lifecycle. Asset Management tracks contracts, financial costs, software licenses, outage indicators, and more for the CI information stored within the BMC® Atrium™ Configuration Management Database (CMDB) application.

BMC Configuration Management distributes software and patches to desktops, servers, and handheld devices, and can synchronize application code and content. Use this tool to help implement part of the ITIL configuration management process.

BMC Configuration Discovery discovers hardware and software and can monitor usage of software. Use this tool to help implement the CMDB data load and the audit parts of the ITIL configuration management process. It can also play a role in the software license compliance part of the Asset Management lifecycle.

The BMC Atrium CMDB product provides all the necessary features to implement a CMDB, including normalization and reconciliation of data. Data normalization uses the Definitive Software Library (DSL).

As part of the BMC Remedy IT Service Management (ITSM) Suite, Asset Management is integrated with BMC Remedy Service Desk (which contains the BMC Remedy Incident Management and BMC Remedy Problem Management applications), BMC Remedy Change Management, and BMC Service Level Management, and offers flexibility to support customized business processes.

To help you understand how the ITIL configuration management processes are supported by BMC applications, this white paper includes:

- Process flow diagrams—for both the high-level overview, and the detailed steps.
- Text explaining how the process is supported by the application.
- Delineation of the process into separate user roles.

Process flow shapes and text indicators

The process flow diagrams in this white paper use the following shapes and text indicators:

Table 1-A: Process flow shapes and text indicators

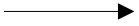
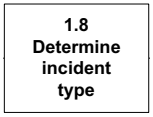
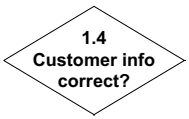
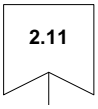
Shape or text indicator	Description
	Start or end shape indicates the starting or ending point of the process flow, for example, change initiation.
	Flow line shape indicates the sequence of steps and the direction of the process flow.
	Action or process shape indicates a single step in the flow, for example, determine incident type.

Table 1-A: Process flow shapes and text indicators (Continued)

Shape or text indicator	Description
	Decision shape indicates a branching point (Yes or No) in the process flow, for example, customer info correct?
	Off-page shape indicates that the process continues in a different diagram; the number indicates the step. For example, process continues in a different diagram with step 2.1.
	Chevron shape indicates that the process started from a different diagram and continues here. For example, process continues from step 2.11.
	Subroutine shape indicates a sequence of actions that perform specific tasks embedded within an external process flow, for example, Incident Management or Change Management.
	Identifies databases used in ITSM 7.0 process flows, for example, service level management or CMDB.

For more information

For information about additional BMC best practices, see the following documentation:

- *BMC Best Practice Process Flows for ITIL Change Management*
- *BMC Best Practice Process Flows for ITIL Incident and Problem Management*

For detailed information about the ITSM 7.0 applications, see the following documentation:

- *BMC Remedy Asset Management 7.0 User's Guide*
- *BMC Remedy Service Desk: Incident Management 7.0 User's Guide*
- *BMC Remedy Service Desk: Problem Management 7.0 User's Guide*
- *BMC Remedy Change Management 7.0 User's Guide*

For information about other BMC applications mentioned in this white paper, see the following documentation:

- *BMC Atrium CMDB 2.0 User's Guide*
- *BMC Configuration Management Introduction to Products 7.0 Guide*

For additional information about the relationship between Asset Management, ITIL, and the CMDB, see the following BMC white paper:

- *Asset Management, ITIL®, and the CMDB: Connecting the Dots between IT Operations and the Bottom Line*

Chapter 2

ITIL configuration management

ITIL configuration management process is responsible for controlling all managed IT infrastructure items and for maintaining the CMDB. BMC supports ITIL configuration management with the following applications:

- **BMC Remedy Asset Management**—Lets IT professionals track and manage enterprise configuration items (CIs)—and their changing relationships—throughout the entire asset lifecycle. For details of the extended functionality for asset management that it provides, see "Asset Management" on page 23.
- **BMC Configuration Management**—Distributes software and patches to desktops, servers, and handheld devices, and can synchronize application code and content.
- **BMC Configuration Discovery**—Discovers hardware and software and can monitor usage of software. Use this tool to help implement the CMDB data load and the audit parts of the ITIL configuration management process.
- **The BMC Atrium CMDB**—Provides all the necessary features to implement a CMDB, including normalization and reconciliation of data. Data normalization uses the Definitive Software Library (DSL).

The ITIL Configuration Management process flow includes the following user roles:

Table 2-A: Configuration Management user roles

Role	Description
Configuration manager	This is a role in ITIL. The configuration manager and the asset manager might be the same person within an organization. The configuration manager controls the CMDB. ITIL includes a separate role for a configuration administrator who administrates the CMDB. Because BMC can automate some of the steps for a configuration administrator, these flow diagrams attach non-automated steps to the configuration manager role.
Configuration auditor	This person audits CIs in the CMDB against the physical items.
Discovery	Some steps of the process are completed or assisted by discovery tools, such as BMC Configuration Discovery.
System	Some steps of the process are completed by the system without manual intervention.
Service support, service delivery, and other related processes	This includes databases and other ITSM processes that interact with the ITIL Configuration Management processes, including: ■ Asset Management ■ Change Management ■ CMDB ■ Incident Management

This section describes the ITIL Configuration Management processes and user roles.

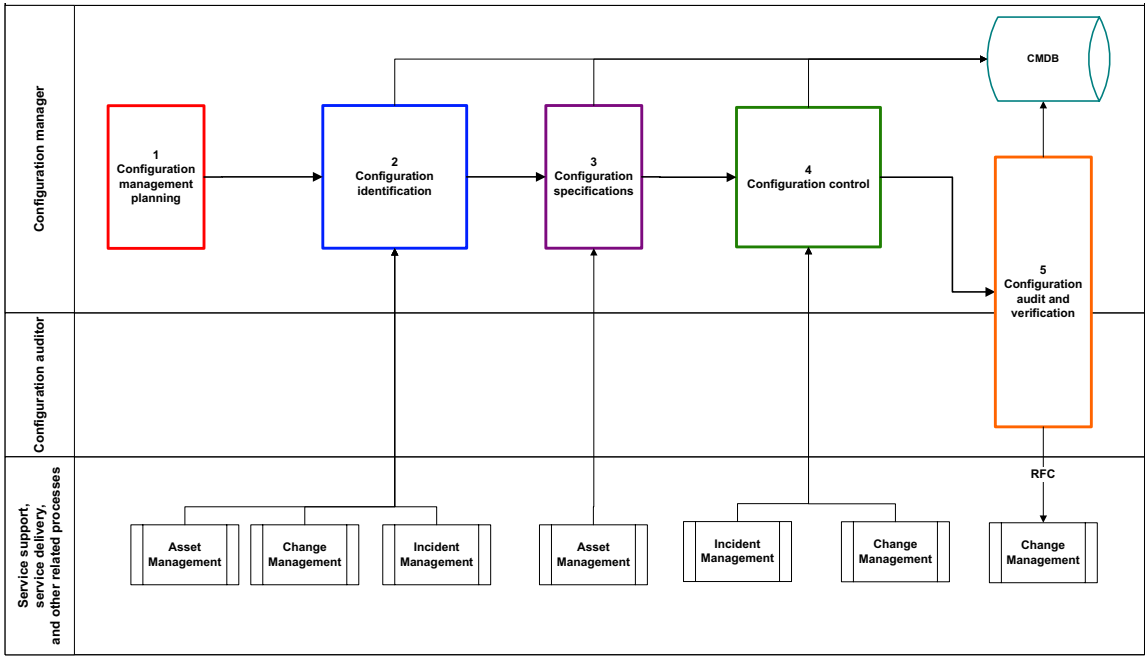
For information about BMC applications that support ITIL Configuration Management, see:

- *BMC Asset Management 7.0 User' Guide*
- *BMC Atrium CMDB 2.0 User's Guide*
- *BMC Configuration Management Introduction to Products 7.0 Guide*

Overview

The configuration management process includes five stages.

Figure 2-A: Overview of the configuration management process



The configuration management process begins when the configuration manager plans the configuration management strategy.

Stage 1 **Configuration management planning**—During this stage, the configuration manager creates the configuration plan, which includes plans for the CMDB. It also includes building the configuration catalog, the product catalog, and DSL entries.

Stage 2 **Configuration identification**—The configuration manager identifies configuration items. New configuration items can be recorded and identified as part of Asset Management, Change Management, or Incident Management.

When a new configuration item is identified, it is stored in the CMDB.

Stage 3 **Configuration specifications**—The configuration manager manages configuration specifications. Configuration specifications are recorded through Asset Management and stored in the CMDB.

Stage 4 **Configuration control**—The configuration manager controls changes to configuration items. Requests for configuration changes come from both incident management and change management. Updates to the configuration are stored in the CMDB.

Stage 5 **Configuration audit and verification**—The configuration manager and the configuration auditor verify configuration changes and perform periodic configuration audits.

Database corrections resulting from this process update the CMDB. If changes are required, a request for change is created and completed by the change management process.

Details

This section describes the detailed steps for each stage of the configuration management process.

Stage 1 Configuration management planning

In this stage, the configuration manager creates and implements a configuration plan. These are manual planning and implementation steps, performed outside of the Asset Management application. The configuration plan includes plans for the CMDB. It also includes building the configuration catalog, the product catalog, and DSL entries.

Planning the CMDB is a key aspect of configuration planning. These plans include:

- Scope, depth, and breadth of the CMDB.
- Method to populate the CMDB. For example, the CMDB can be initially populated from spreadsheets and bulk loads. Plans must include how to normalize and reconcile the initial load.
- Time lines.

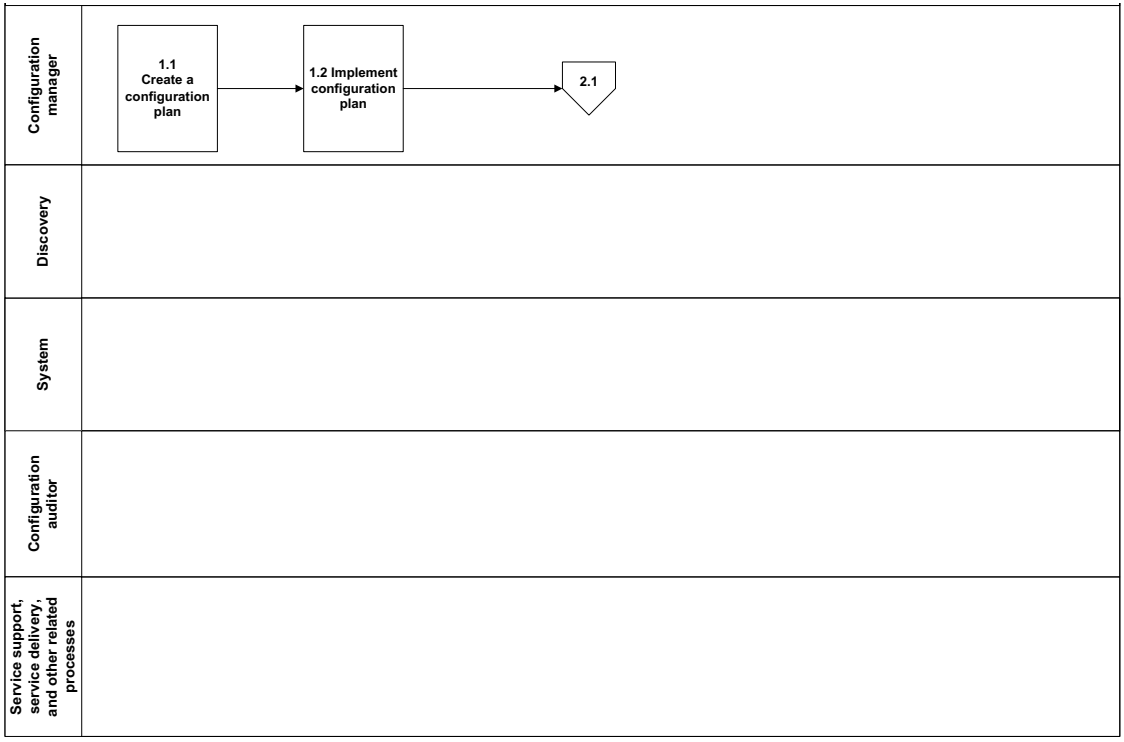
When determining the *scope* of the CMDB, plan which CIs will be tracked in the CMDB, such as servers and software.

When determining the *depth* of the CMDB, plan the number and level of CI relationships to maintain. It is helpful to review CI relationship types and contact relationship types.

When determining the *breadth* of the CMDB, plan the level of detail to be tracked on CIs. It is helpful to review CI attributes, financials, maintenance schedules, and other fields. It is also helpful to review CI impacted areas.

When implementing the plans, the configuration manager defines structures and foundation data that will be used during the identification stage. For example, product categorizations are used to classify the CIs. Foundation data recorded for CIs can include sites, locations, owners, and (if using the multi-tenancy feature of the application) companies.

Figure 2-B: Configuration management planning



The process includes the following steps:

1.1 The configuration manager creates a configuration plan.

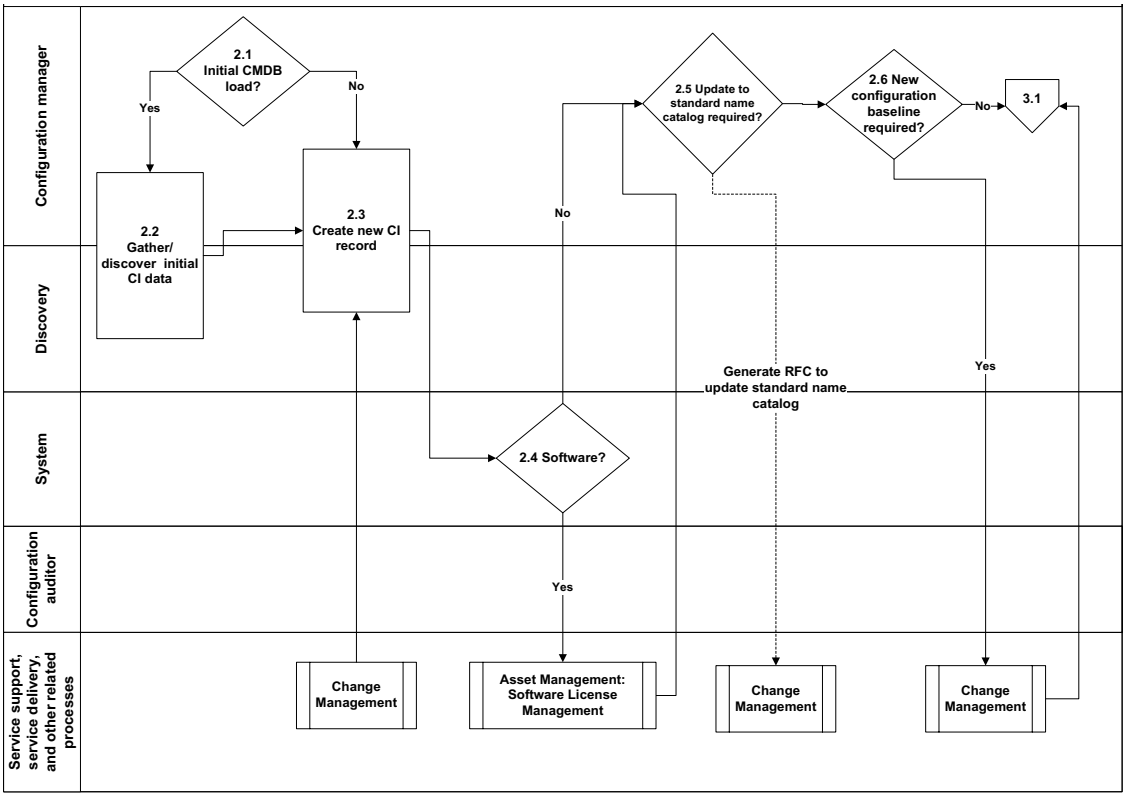
1.2 The configuration manager implements the configuration plan.

The process continues with the Configuration identification stage at step 2.1.

Stage 2 Configuration identification

In this stage, the configuration manager identifies configuration items. Discovery tools can be used to discover and create CI records.

Figure 2-C: Configuration identification



2.1 The configuration manager determines whether to perform an initial CMDB load.

2.2 If this is an initial CMDB load, CI data is gathered or discovered.

This can be automated, or partially automated, by using discovery tools to find CIs. Also, the configuration manager can physically survey the organization and gather CIs.

2.3 The configuration manager or discovery tool creates a new CI record.

The CI record includes product categorization and other foundation data, such as the site, owner, and company.

2.4 The system determines whether the CI is software.

For software CIs, the system follows the Asset Management process for Software License Management, as described in "Software license management—license compliance" on page 35.

2.5 The configuration manager determines whether an update to the standard name catalog is required.

Standardized names for products are provided by the product catalog. To update this catalog, the asset manager generates an RFC to update the catalog. This update is handled by the change management process.

2.6 The configuration manager determines whether a new configuration baseline is required.

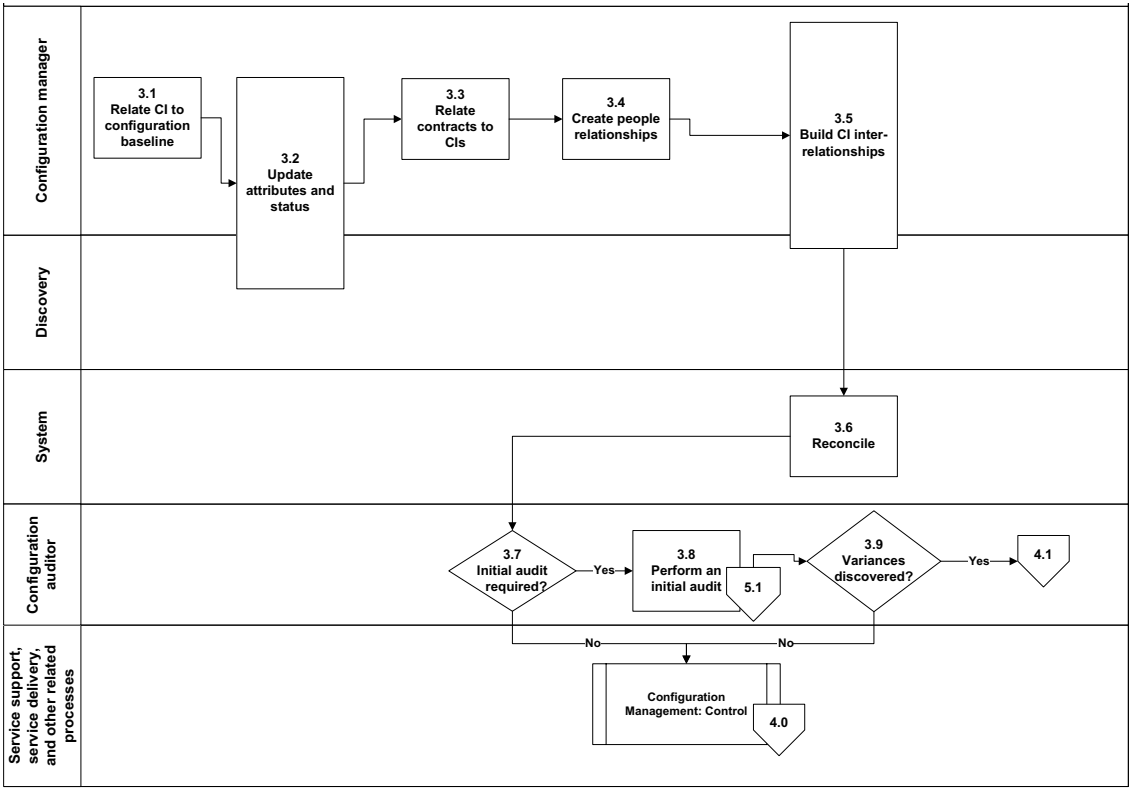
If a new configuration baseline is required, this is handled through the change management process.

The process continues with the Configuration specification stage at step 3.1.

Stage 3 Configuration specification

In this stage, the configuration manager relates the CI to the configuration baseline and records attributes. At the end of this process, the new CIs might be audited.

Figure 2-D: Configuration specification



3.1 The configuration manager relates the CI to the configuration baseline.

3.2 The configuration manager updates the attributes and status of the CI.

If discovery tools initially found the CI, some of the attributes might be populated by the tools.

3.3 The configuration manager relates contracts to CIs.

The contracts are managed by the Asset Management process for Contract Management, as described in "Contract management" on page 33.

3.4 The configuration manager relates the CI to people.

If you have Incident Management, when support staff look at an incident ticket for that person, the CIs related to that person are displayed.

3.5 The configuration manager relates CIs to each other.

When discovery tools find a CI, they might create relationships to other CIs.

3.6 The system reconciles the CI.

The Reconciliation Engine, part of the BMC Atrium CMDB, reconciles CIs from multiple sources. Up until this point, you are working in the discovery data set or the asset sandbox data set. You can configure which source is the standard when there are conflicts.

3.7 The configuration auditor determines whether an initial audit is required.

If an audit is not required, the process moves to the control stage. At this point, it is in a holding state, which you can think of as step 4.0—when an action occurs that requires the CI to be updated, the process starts with 4.1.

3.8 If an audit is required, the configuration auditor performs the initial audit.

Details of the audit process are described in "Configuration audit and verification" on page 20.

3.9 The configuration auditor determines whether variances are discovered.

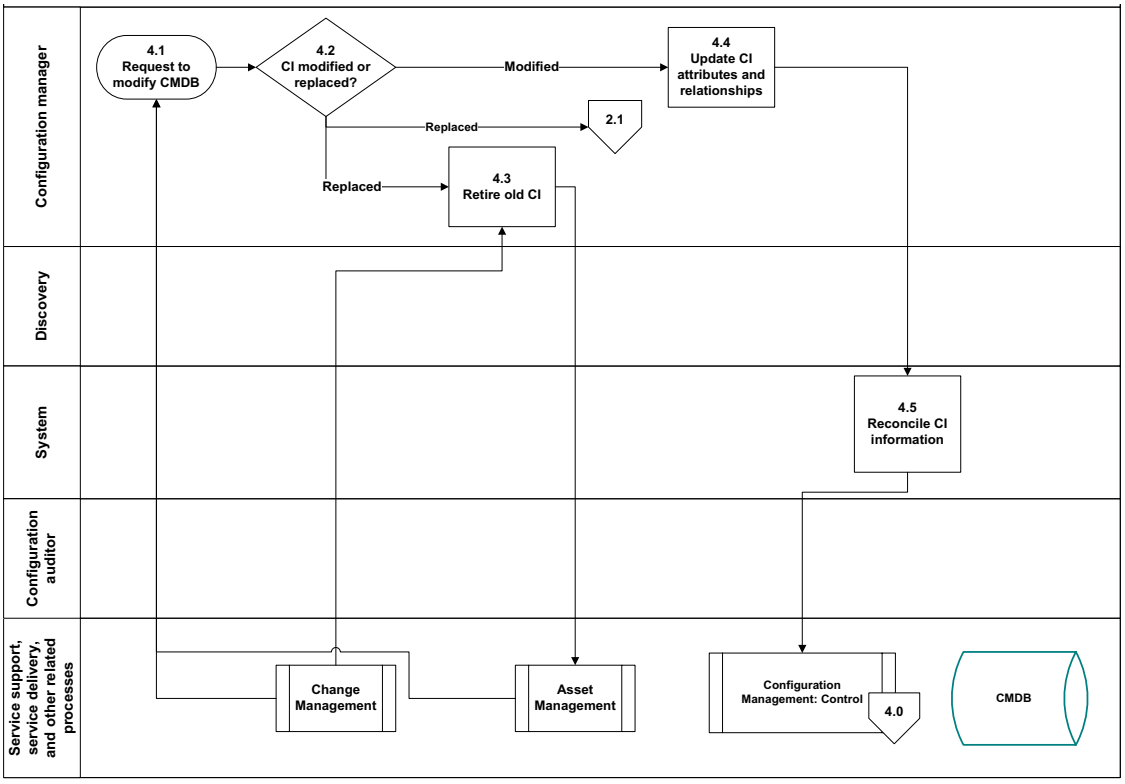
If variances are discovered, the process moves to the configuration and control stage with step 4.1.

Otherwise, the process moves to the control stage, but is on hold until an action occurs that requires the CI to be updated.

Stage 4 Configuration control

In this stage, the configuration manager responds to requests to modify the CMDB.

Figure 2-E: Configuration control



4.1 The configuration manager receives a request to modify the CMDB.

This request can come from either the Change Management or Asset Management process.

4.2 The configuration manager determines whether the CI has been modified or replaced.

4.3 If the CI has been replaced, the configuration manager retires the old CI.

This starts the asset management process for retiring CIs. Also the configuration management process returns to the identification stage with step 2.1.

4.4 If the CI has been modified, the configuration manager updates the CI attributes and relationships.

4.5 The system reconciles the CI against other sources that add, modify, and delete CIs.

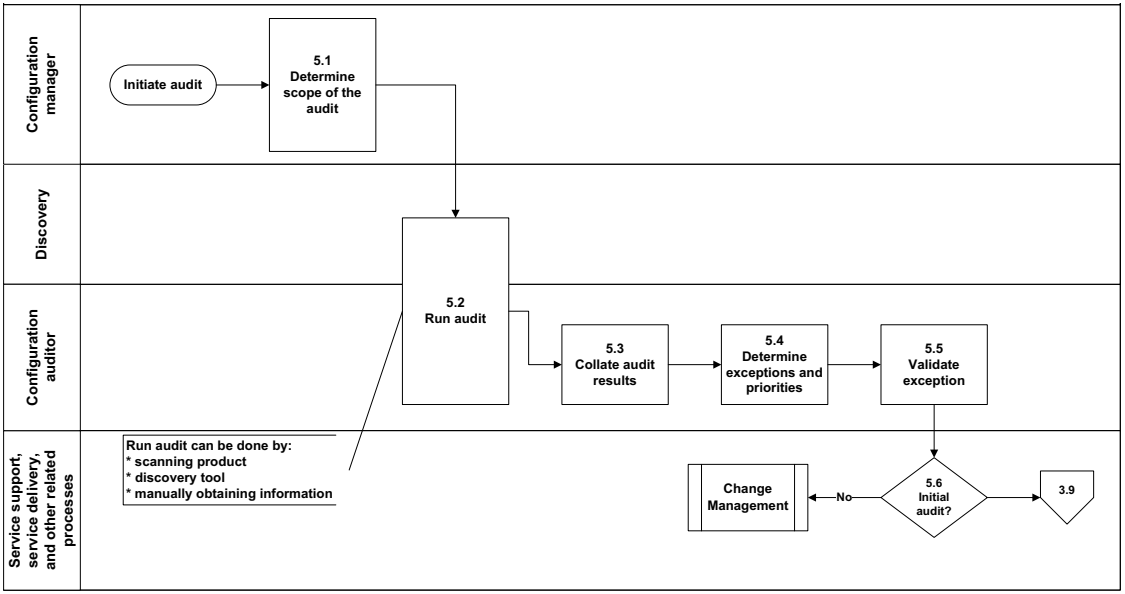
The Reconciliation Engine, part of the BMC Atrium CMDB, reconciles CIs from multiple sources. You can configure which source is the standard when there are conflicts.

The process of modifying the CI is complete, and the control process moves to a holding state, which you can think of as step 4.0—when an action occurs that requires the CI to be updated, the process starts again with 4.1.

Stage 5 Configuration audit and verification

In this stage, the configuration manager initiates an audit, which is performed by the configuration auditor. An audit is a comparison between CIs recorded in the CMDB and the physical items.

Figure 2-F: Configuration audit and verification



This process begins when the configuration manager initiates an audit. The process continues with the following steps:

5.1 The configuration manager determines the scope of the audit.

5.2 The configuration auditor runs the audit.

An audit can be performed by:

- Scanning the product.

  A selective or full inventory can be performed with a bar-code reader.

- Using a discovery tool.
- Manually obtaining the information.

5.3 The configuration auditor collates the audit results.

The configuration auditor starts to analyze the results of the audit.

5.4 The configuration auditor determines exceptions and priorities.

5.5 The configuration auditor validates exceptions.

5.6 If this is an initial audit, the process returns to the configuration specification stage with step 3.9. Otherwise, the exceptions are handled by the change management process.

Chapter

3 Asset Management

Asset management extends the CMDB functionality to provide processes for "cradle-to-grave" asset management.

The asset management process flows include the following user roles:

Table 3-A: Asset Management user roles

Role	Description
Asset manager	Manages assets throughout their lifecycle. Other asset users take on one or more of the other roles, depending on their responsibilities.
Business manager	Manages the business needs of the organization.
Configuration auditor	Audits CIs in the CMDB against the physical items.
Financial manager	Responsible for managing asset costs.
IT support	People who deploy and maintain assets. It also refers to people who provide support within the change management, incident management, and problem management processes.
Manager	Someone in a managerial role, but not necessarily an asset manager or a business manager.

Table 3-A: Asset Management user roles (Continued)

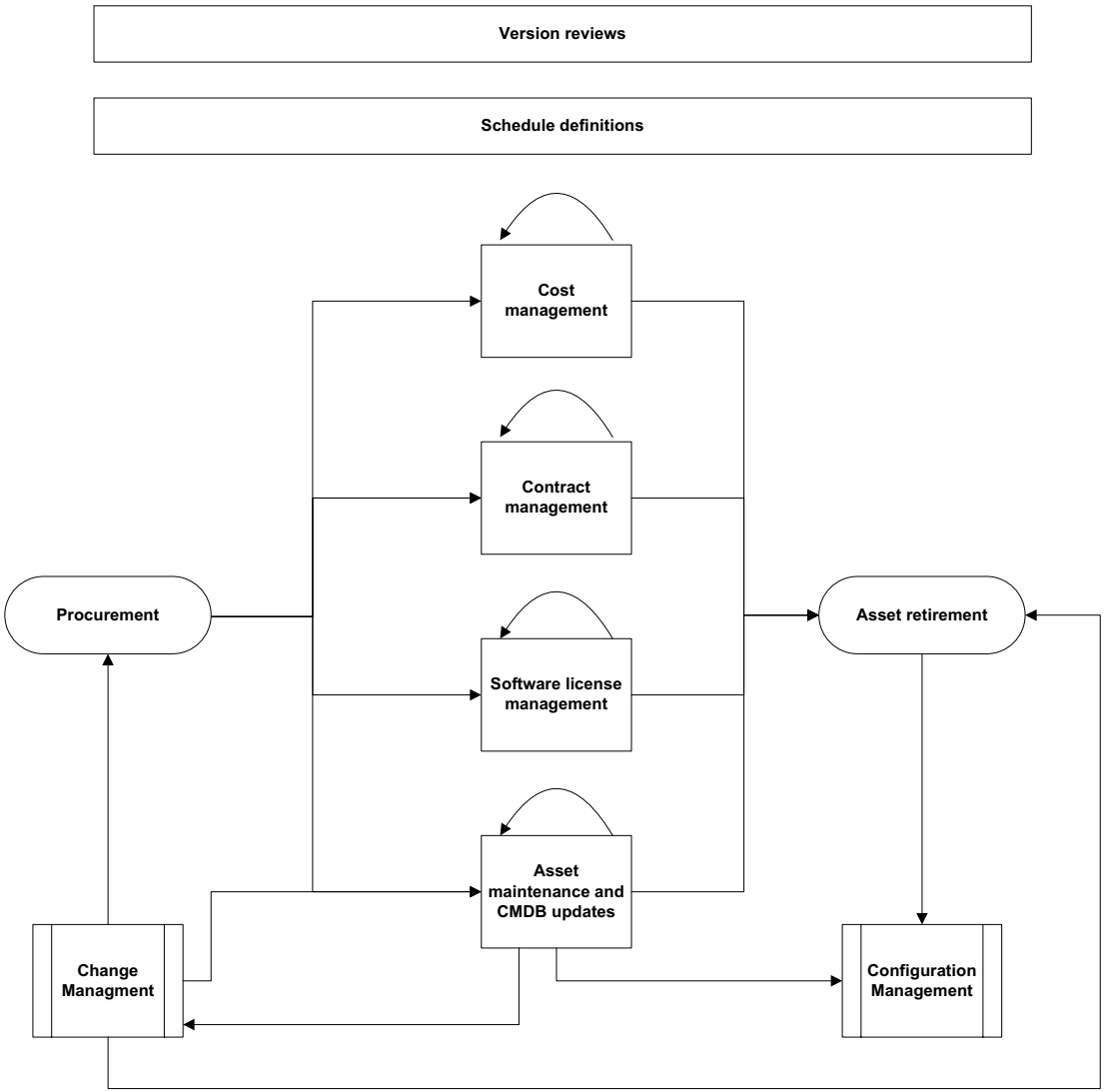
Role	Description
Purchasing	Responsible for procuring assets.
Receiving	Responsible for receiving incoming assets.
Requester	Someone requesting an asset. This could be a member of IT staff, or anyone in the organization.
System	Some steps of the process are completed by the system without manual intervention.
Service support, service delivery, and other related processes	Includes databases and other ITSM processes that interact with the asset management process, including: ■ Asset management (and specific processes within asset management) ■ CMDB ■ Change management ■ Configuration management ■ Incident management ■ Problem management

This section describes the Asset Management processes and user roles. For information about using the application, see the *BMC Remedy Asset Management 7.0 User's Guide*.

Overview

The asset management process flow describes the lifecycle of the asset.

Figure 3-A: Asset lifecycle overview



The asset lifecycle starts with procurement and ends with retirement of the asset. The change management process determines when assets are procured and can control when they are retired. When an asset is retired, the configuration management process updates the CMDB.

Between procurement and retirement, the asset management includes the following repeating processes:

- Cost management
- Contract management
- Software license management
- Asset maintenance and CMDB updates

Version reviews and schedule definitions apply to the entire lifecycle of assets. Version reviews indicate the review of hardware and software versions.

Schedule definitions indicate production scheduling. These include definitions for the following schedules and windows:

- **Blackout windows**—Used by asset management, this is the time when a CI must not be brought down. For example, the server used by payroll might have a blackout window when paychecks are processed. This is stored in a time segment. This is used by supporting products, such as Change Management.
- **Maintenance windows**—Used by asset management, these indicate the best time to bring down a system for work. They are stored in time segments. When a CI is *available*, it is available for outages (for example, to perform maintenance). In the maintenance window, when a CI is *unavailable*, it is unavailable for outages. This process is used by supporting products, such as Change Management.
- **Maintenance schedules**—These determine how often maintenance should occur. For example, a particular computer system might need monthly or annual maintenance. If the maintenance requires bringing down the system, the maintenance window and blackout window determine when the CI can and cannot be brought down to perform the work. The maintenance schedules generate a change request to schedule maintenance.
- **Audit schedules**—Used by asset management, these are not stored in time segments. The audit schedule generates a change request to schedule the audit.

ITSM also includes the following features to account for CI availability:

- **Scheduled outages**—Used by change management, a CI is brought down and unavailable to users during this time. This should happen within a maintenance window.
- **Schedule of changes**—Used by change management, scheduled changes might not include down time, for example if the CI can be running during the change. It is not stored in time segments.
- **Unscheduled outages**—Incident management can indicate CI unavailability, which indicates that a CI is unavailable or partially unavailable to users. These are not tracked as scheduled items.

Details

Because of the overall flow of the asset management processes, the individual flows are not assigned to numbered stages.

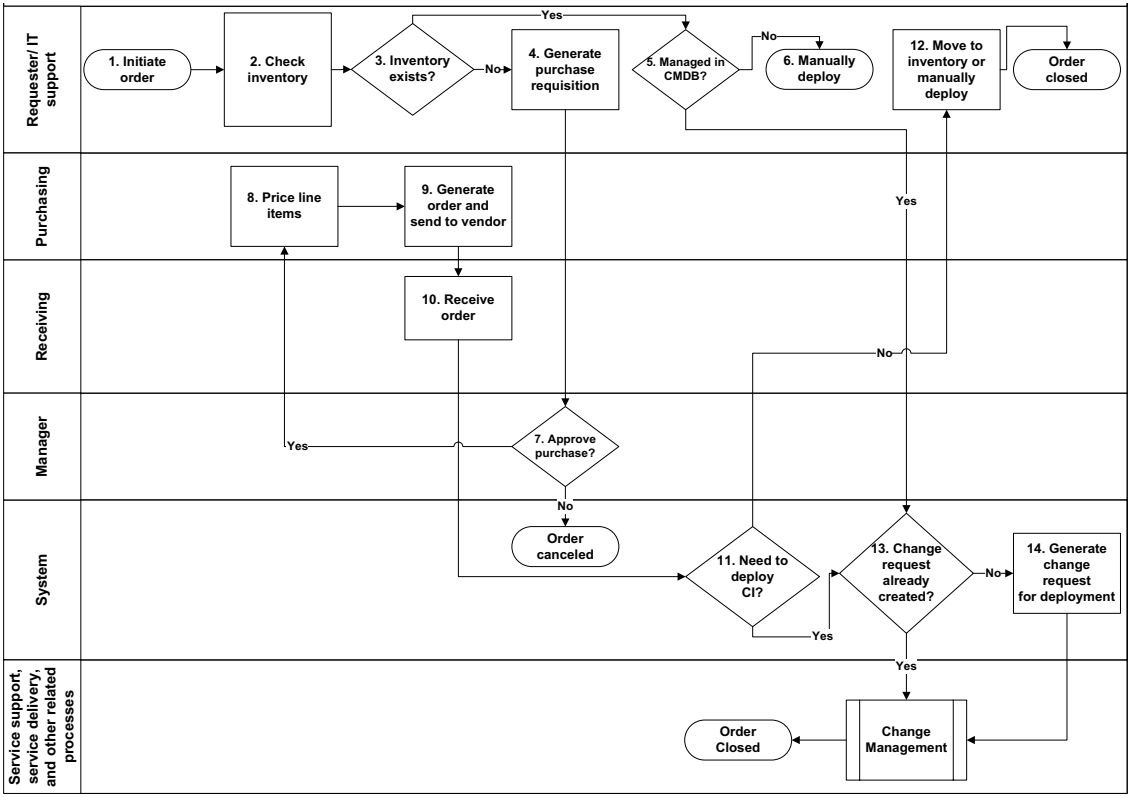
This section includes the following process flows:

- "Asset retirement" on page 42
- "Version reviews" on page 43
- Schedule definitions, which consists of:
  - "Schedule definitions—maintenance windows" on page 44
  - "Schedule definitions—blackout windows" on page 45
  - "Schedule definitions—maintenance schedules" on page 46
  - "Schedule definitions—audit schedules" on page 47

Procurement

The procurement process starts the asset lifecycle. In this stage, a requester initiates the process. The process continues with input from purchasing, receiving, and management until the order is either closed or canceled.

Figure 3-B: Procurement



1. The requester initiates the order.
2. The IT support checks inventory.
3. IT support determines whether the item is in inventory.

   If the item is in inventory, a purchase order is not created.
4. If the item is not available, the requester generates a purchase order.

   The process continues with step 7.
5. If the item is available, IT support evaluates whether the item is managed by the CMDB.

   Items managed by the CMDB are controlled by the change management process. For items managed by the CMDB, the process continues with step 13.
6. If the item is not managed by the CMDB and is in inventory, IT support deploys the item.

   For example, if mice are managed as bulk items in inventory, but not managed by the CMDB, after checking inventory, IT support takes the mouse out of inventory without further interaction with the application.
7. When a purchase order is created, it is sent to a manager for approval.

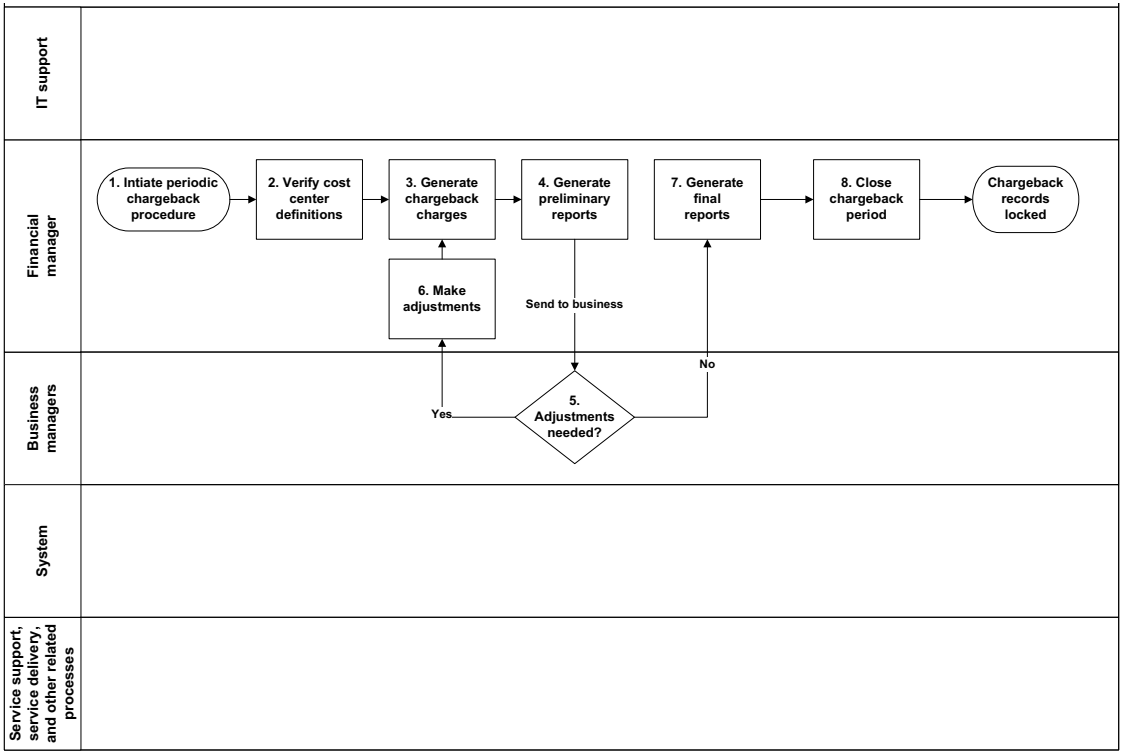
   If the manager does not approve the purchase order, the order is canceled.
8. If the purchase order is approved, purchasing prices the line items.
9. Purchasing generates an order and sends it to the vendor.
10. When the order arrives, receiving processes the item.
11. The system determines whether the item must be deployed as a CI.
12. If the item is not deployed as a CI, it is either moved to inventory or manually deployed, completing the order process.
13. If the item is deployed as a CI and managed by the CMDB, the system determines whether a change request has been created for the item.

    If a change request has been created, the change management process manages deployment of the CI, and the order is completed.
14. Otherwise, the system creates the change request, which is managed by the change management process.

Cost management—chargebacks

The financial manager, with feedback from the business managers, performs the chargeback process of cost management.

Figure 3-C: Cost management—chargebacks



1 The financial manager initiates the periodic chargeback procedure.

2 The financial manager verifies the cost center definitions.

3 The financial manager generates the chargeback charges.

4 The financial manager generates the preliminary reports.

These reports are sent to the business manager to review.

5 The business manager analyzes the reports and determines if any adjustments to the charge back charges are needed.

6 If an adjustment is needed, the financial manager makes the adjustment, then returns to step 3.

7 If no adjustments are required, the financial manager generates the final reports.

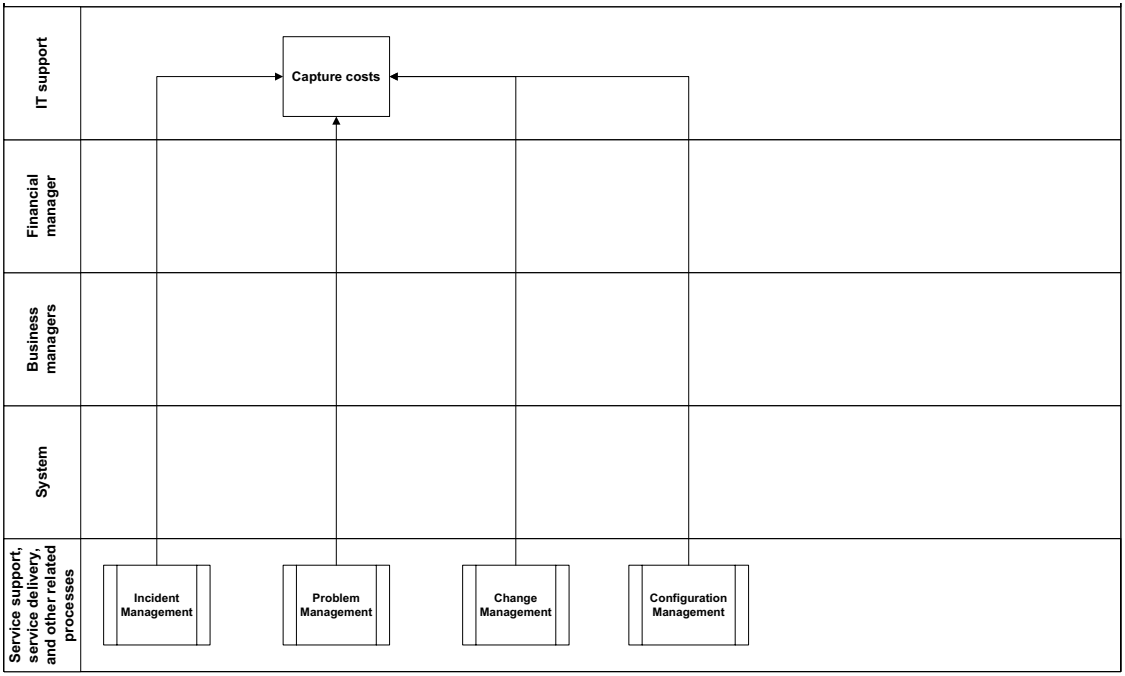
8 The financial manager then closes the chargeback period.

After the chargeback period is closed, the chargeback records are locked.

Cost management—cost capture

In this process, IT support captures costs based on reports from the incident management, problem management, change management, and configuration management processes.

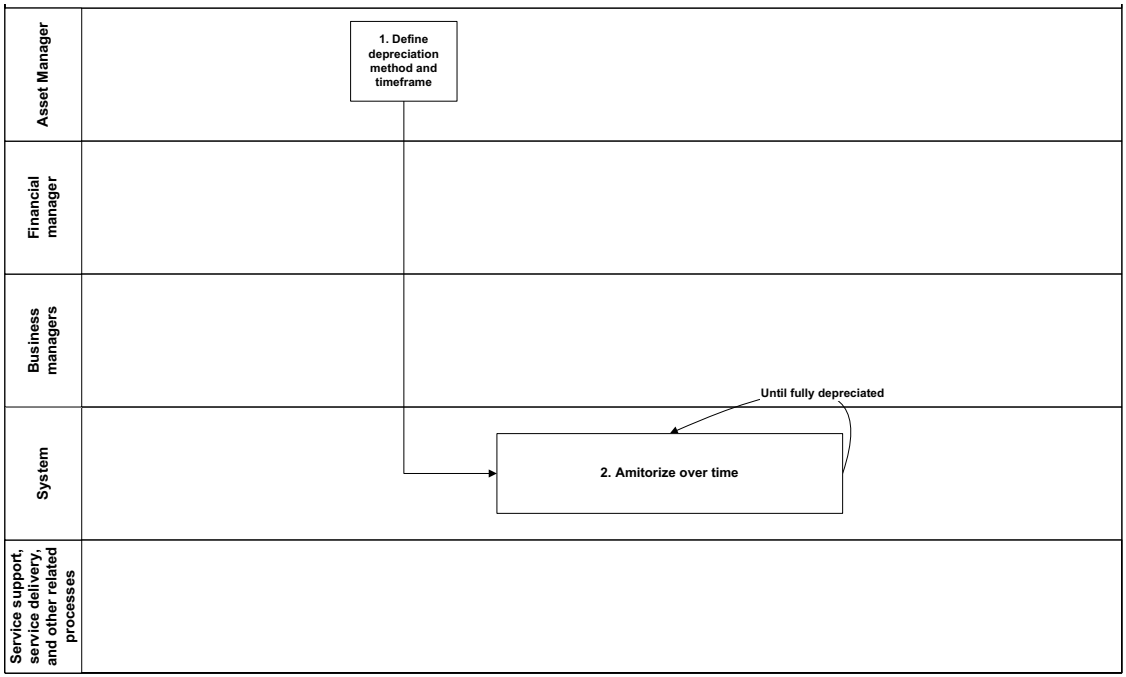
Figure 3-D: Cost management—cost capture



Cost management—depreciation

The asset manager defines the terms of depreciation, which run automatically by the system.

Figure 3-E: Cost management—depreciation



1 The asset manager determines which method of depreciation to use and the timeframe over which to use it.

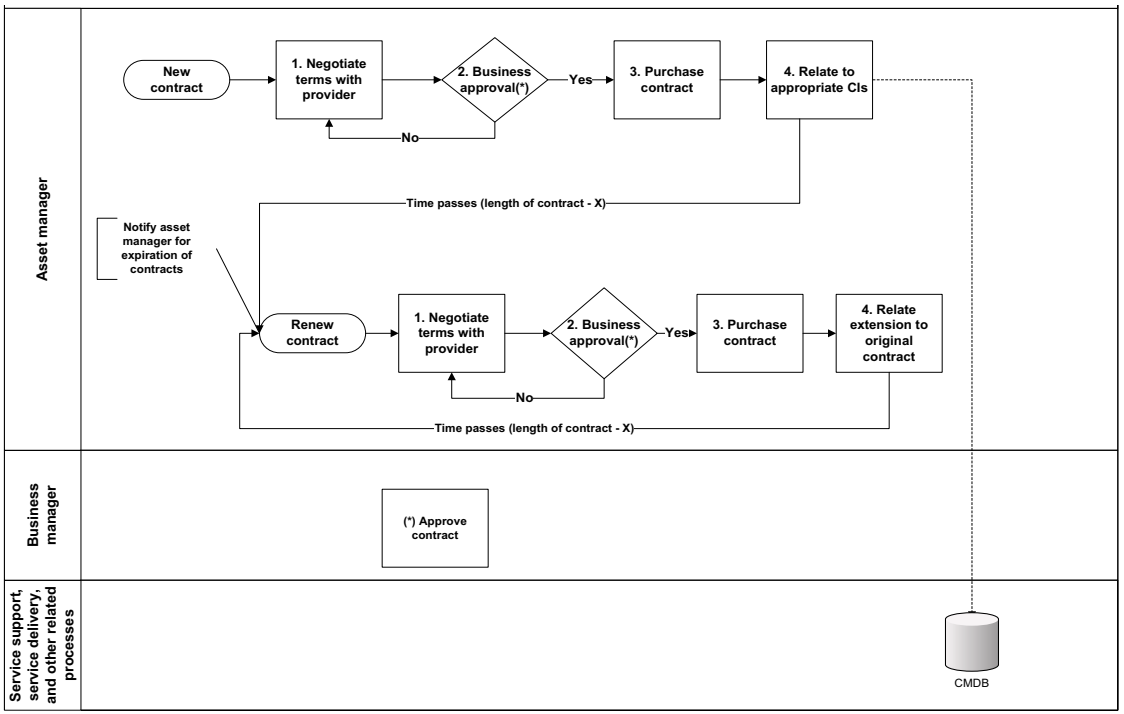
2 The asset is amortized over the specified timeframe.

The amortization continues regularly until the asset is fully depreciated.

Contract management

In this process, the asset manager oversees the purchase and renewal of contracts with providers, with approval by the business manager. This is an iterative process for each contract. The interval at which the process repeats depends on the length of the given contract.

Figure 3-F: Contract management



Contract management includes both processes for both new and renewed contracts.

New contract process

1 The asset manager negotiates the terms of the new contract with the provider.

2 The asset manager seeks business approval from the business manager.

If the terms are not acceptable, the asset manager returns to step 1 to renegotiate the terms.

3 If the business manager approves the terms, the asset manager purchases the contract from the provider.

4 The asset manager relates the contract to the appropriate CIs and makes sure this is recorded in the CMDB.

After the passage of time (equivalent to the length of the contract minus the period of time required to renegotiate), the asset manager is notified that a given contract is about to expire, which triggers the contract renewal process.

Contract renewal process

The contract renewal process starts when the asset manager is notified of contracts about to expire.

1 The asset manager negotiates the terms of the contract renewal with the provider.

2 The asset manager seeks business approval from the business manager.

If the terms are not acceptable, the asset manager returns to step 1 to renegotiate the terms.

3 If the business manager approves the terms, the asset manager purchases the contract from the provider.

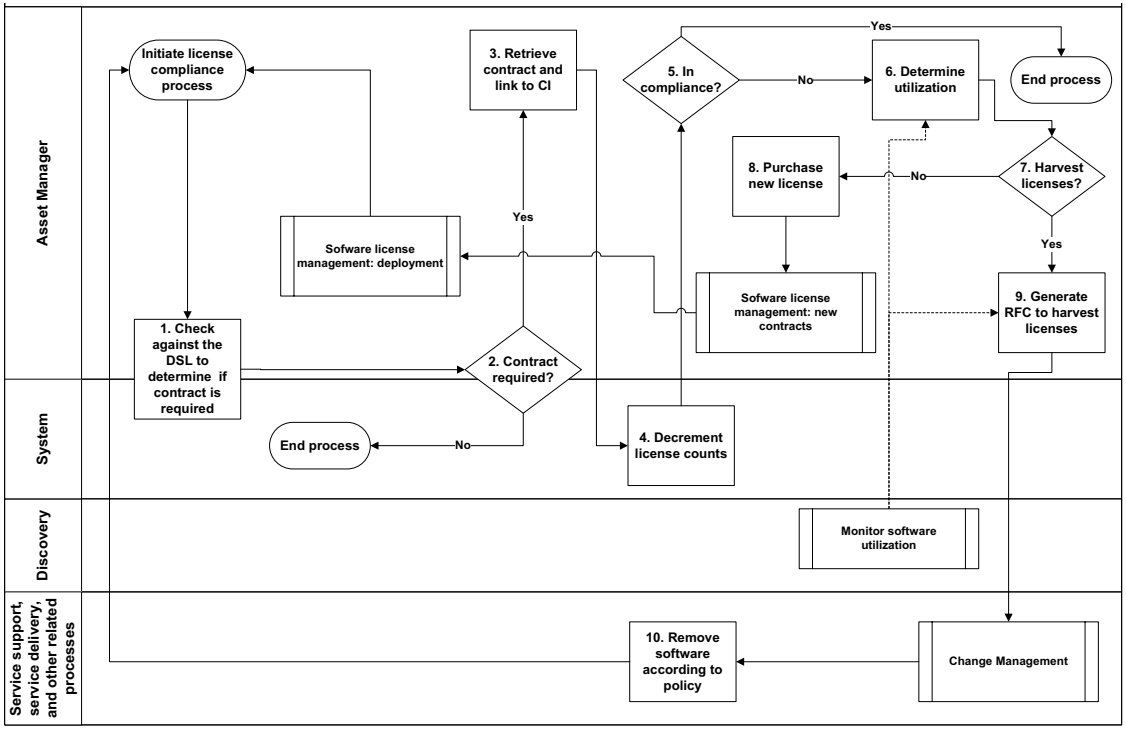
4 The asset manager relates the extended contract to the original contract.

After the passage of time (equivalent to the length of the contract minus the period of time required to renegotiate) the asset manager is notified that a given contract is about to expire, and the process returns to step 1.

Software license management—license compliance

In this process, the asset manager manages software license compliance.

Figure 3-G: Software license management—license compliance



The software license compliance process is initiated when software is deployed or removed.

1 The asset manager checks against the definitive software library (DSL) to determine whether a contract is required.

   This step can be performed by the system.

2 The asset manager or the system determine whether a contract is required.

   If no contract is required, the process ends.

3 If a contract is required, the Asset Manager links the CI to the software contract.

4 The system decrements the number of available licenses remaining.

5 The asset manager determines whether the organization is still in compliance with the license agreement.

If there are sufficient licenses, the process ends.

If the organization is no longer in compliance, the asset manager continues the process to resolve the compliance issue.

6 The asset manager determines utilization of the software.

Tools, such as BMC Discovery Configuration, monitor software usage. The asset manager can use information from this tool to determine utilization.

7 Based on utilization, the asset manager determines whether licenses are available to be harvested.

8 If all licenses are in use, the asset manager purchases a new license.

The asset manager follows the new contract process to purchase the new license, and then deploys the license by following the deployment process.

9 If licenses are available to be harvested, the asset manager generates an RFC to harvest the licenses.

The asset manager can use tools, such as BMC Configuration Discovery, to measure which licenses are unused or least used. This data is helpful in deciding which licenses to harvest. The change management process manages the request.

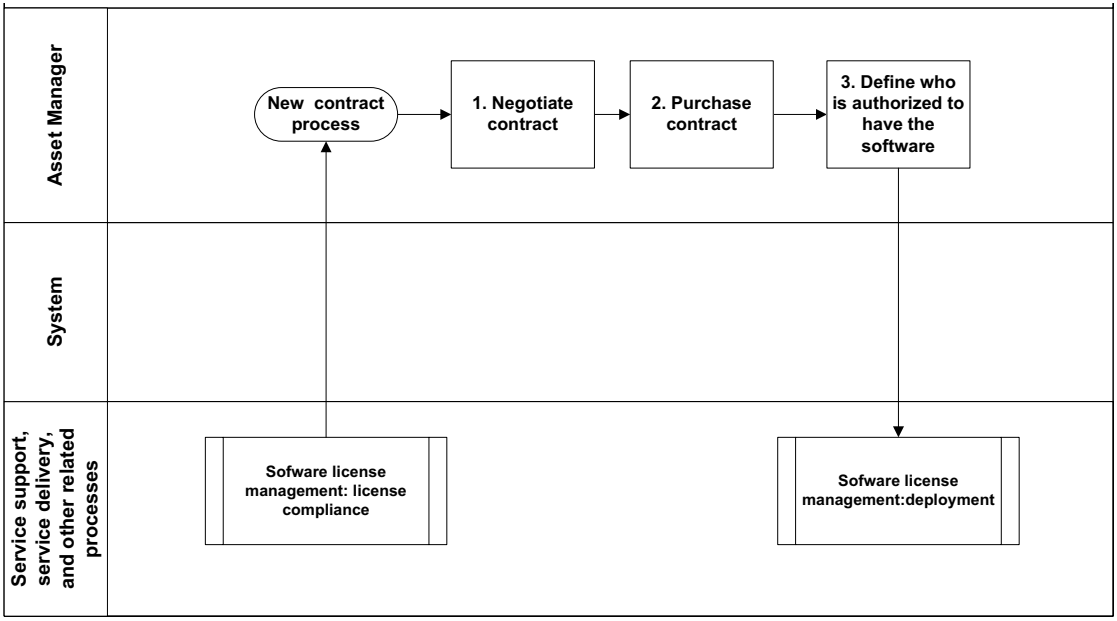
10 The software is removed according to policy.

BMC Configuration Management can be used to remove software according to policy.

Software license management—new contracts

In this process, the asset manager manage new software license contracts.

Figure 3-H: Software license management—new contracts



The new contract process is initiated by the software license compliance process.

1 The asset manager negotiates the contract.

2 The asset manager purchases the contract.

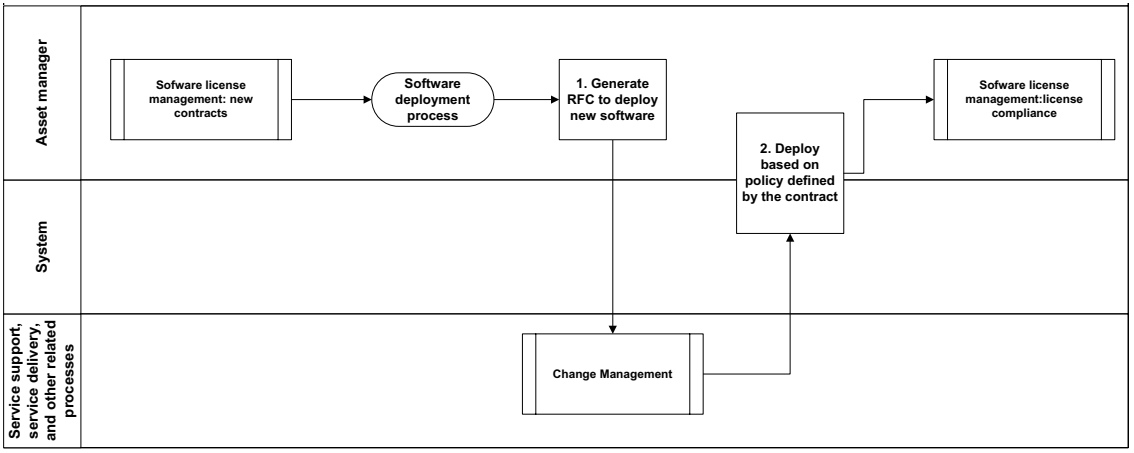
3 The asset manager defines who is authorized to have the software.

At this point, the asset manager can deploy the software.

Software license management—deployment

The asset manager performs the software deployment process.

Figure 3-I: Software license management—deployment



The deployment process is initiated by the new contract process.

1 The asset manager generates an RFC to deploy new software.

The change management process manages the request.

2 The asset manager deploys the software based on the policy defined by the contract.

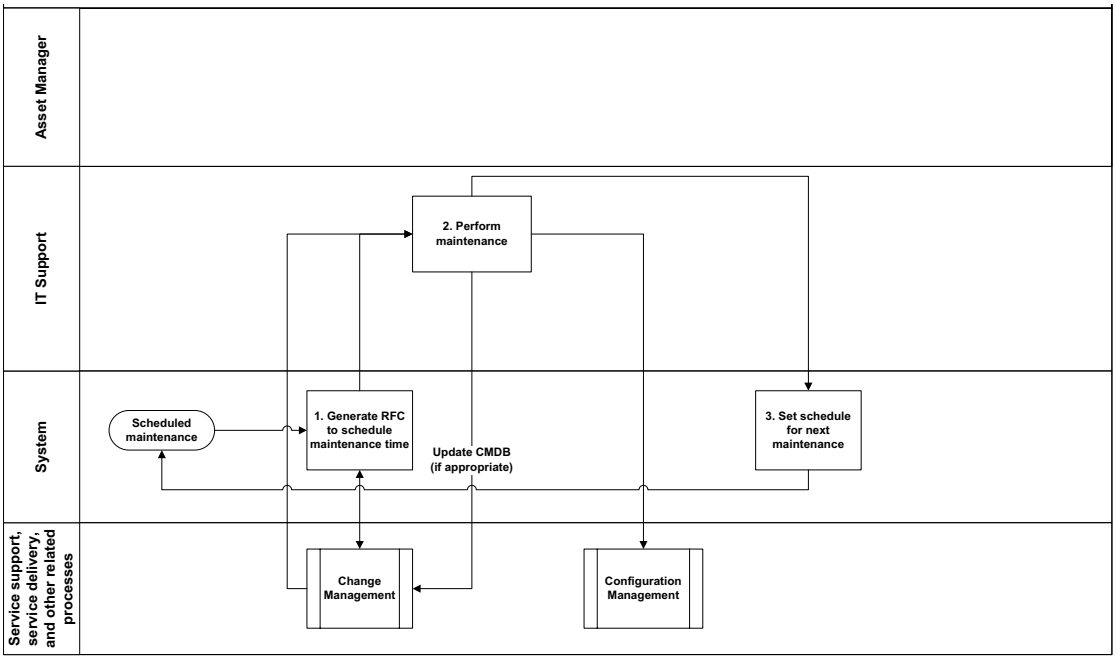
BMC Configuration Management can be used to automate this step.

At this point, the asset manager performs license compliance.

Asset maintenance and CMDB updates—scheduled maintenance

IT support performs maintenance in response to system activity and other processes.

Figure 3-J: Asset maintenance and CMDB updates—scheduled maintenance



1 When scheduled maintenance is set to occur, the system generates an RFC to schedule maintenance time.

   The change management process schedules the maintenance activity.

2 IT support performs maintenance.

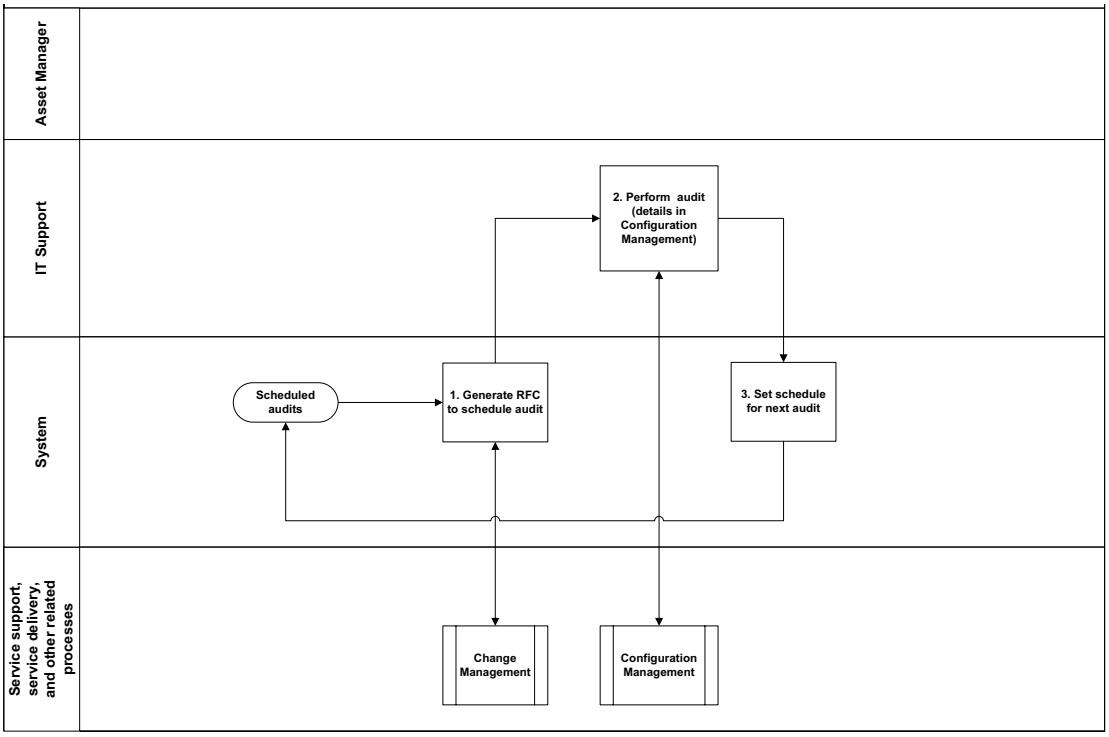
   If an update to the CMDB is required as a result of maintenance, the change management process evaluates the update, and the configuration management process performs the update.

3 When maintenance is complete, the system sets the schedule for the next maintenance.

Asset maintenance and CMDB updates—scheduled audits

IT support performs scheduled audits in response to system activity and other processes.

Figure 3-K: Asset maintenance and CMDB updates—scheduled audits



1 When a scheduled audit is set to occur, the system generates an RFC to schedule an audit.

   The change management process schedules the audit activity.

2 IT support performs the audit.

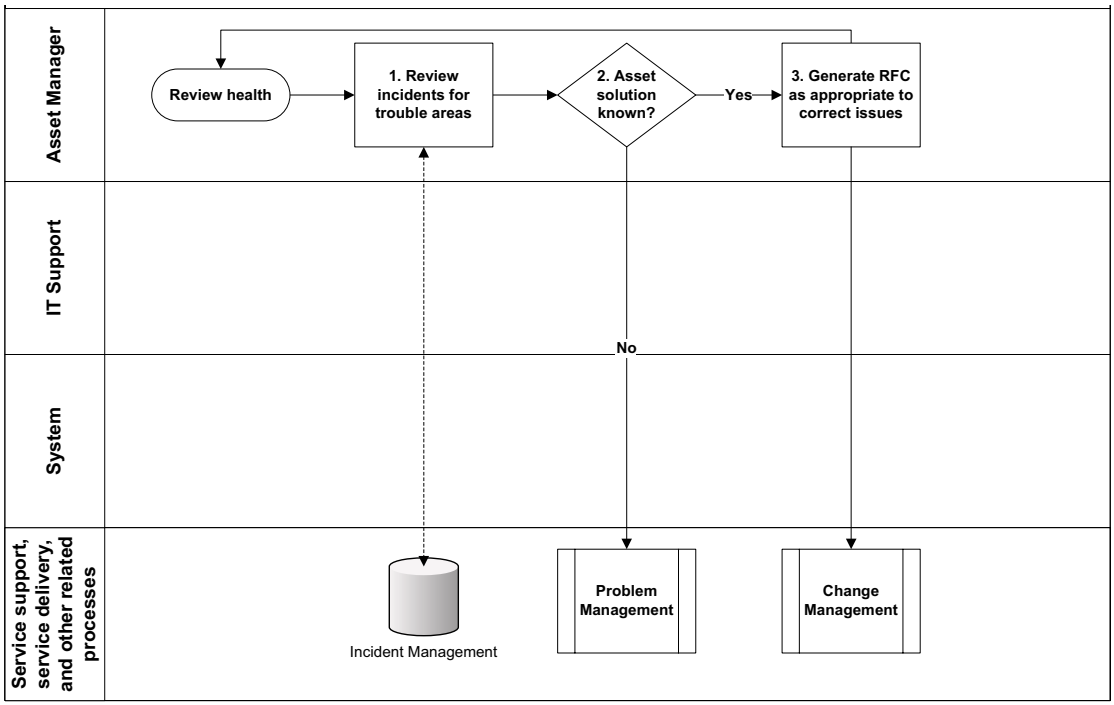
   For details, see "Configuration audit and verification" on page 20.

3 When the audit activity is successfully completed, the system sets the schedule for the next audit.

Asset maintenance and CMDB updates—review health

The asset manager reviews the health of assets and the CMDB. The asset manager can review reports from incident management. If incidents are recorded against an asset, this might be a symptom that the asset should be upgraded, replaced, or retired.

Figure 3-L: Asset maintenance and CMDB updates—review health



1. The asset manager reviews incidents for assets that have issues.
2. The asset manager determines whether the solution is known.

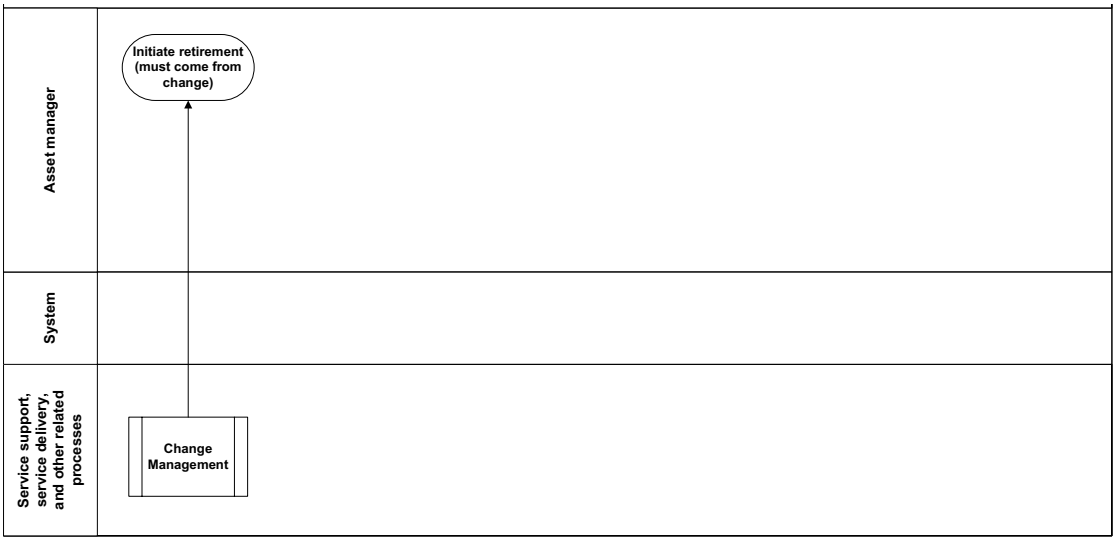
   If the solution is not known, the asset manager creates a problem investigation, to be resolved by the Problem Management process.
3. If the solution is known, the asset manager generates an RFC to correct the issue.

   The change management process completes the change.

Asset retirement

The asset manager retires assets, as initiated by the change management process.

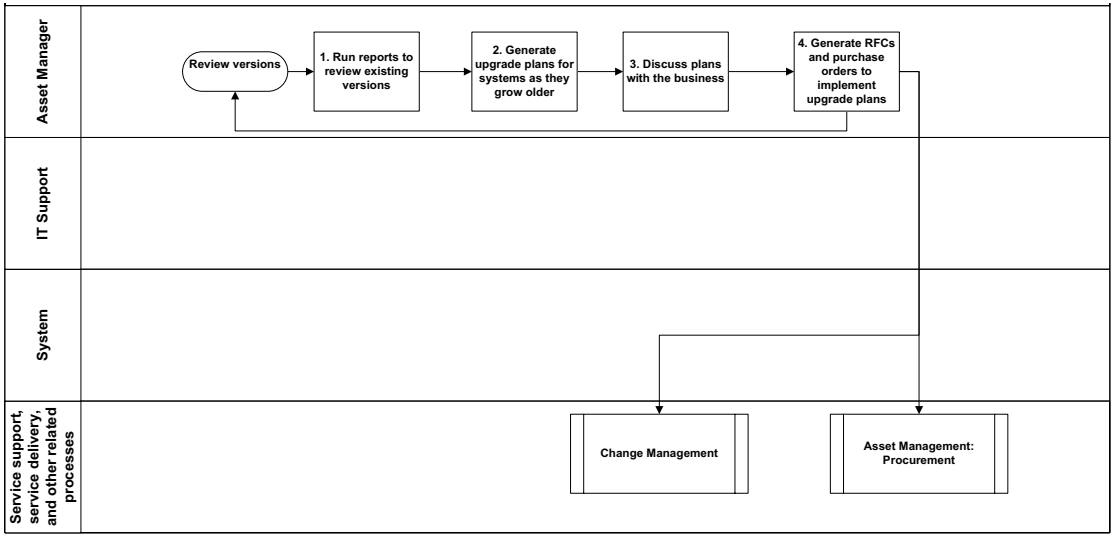
Figure 3-M: Asset retirement



Version reviews

The asset manager performs reviews of software and hardware versions. For example, if support ends for a particular version of a product, the asset manager analyzes the exposure and plans for changes.

Figure 3-N: Version reviews



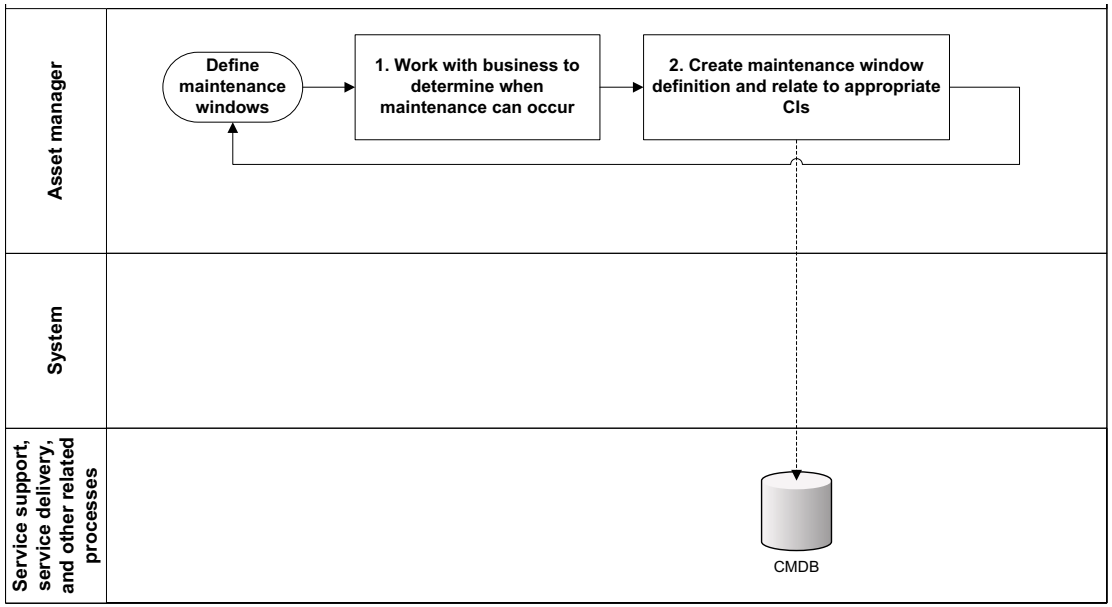
1. The asset manager runs reports to review existing versions.
2. The asset manager generates upgrade plans for systems as they grow older.
3. The asset manager discusses plans with the business.
4. The asset manager generates RFCs and purchase orders to implement upgrade plans.

   RFCs are handled by the change management process. Purchase orders are handled by the asset management procurement process.

Schedule definitions—maintenance windows

The asset manager defines maintenance windows. Maintenance windows indicate the best time to bring down a system for work.

Figure 3-O: Schedule definitions—maintenance windows



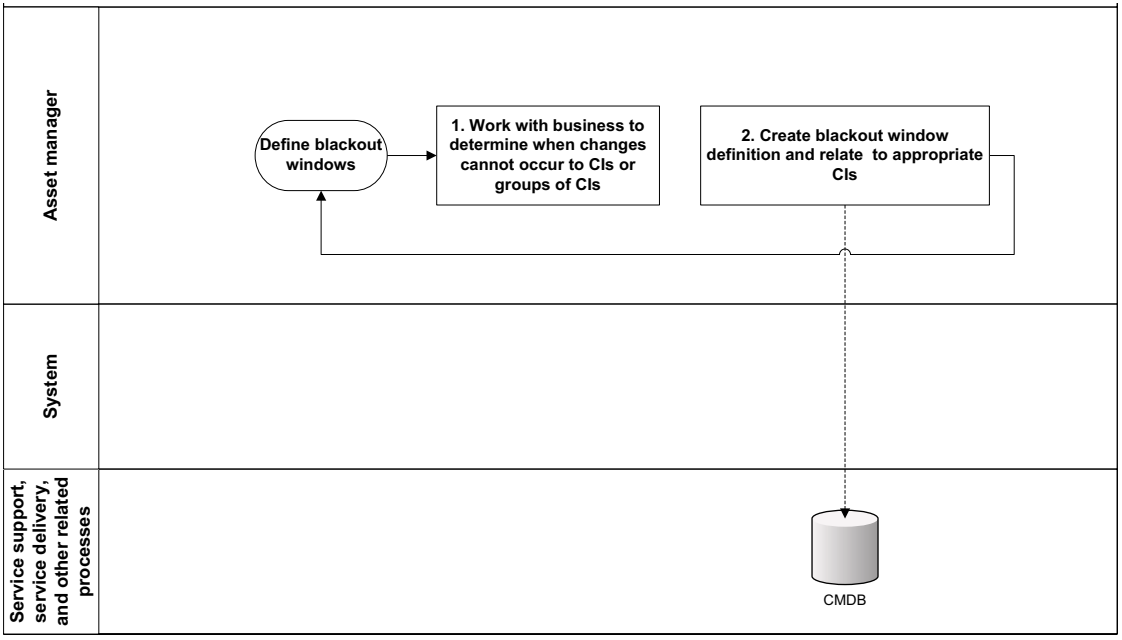
1. The asset manager works with business to determine when maintenance can occur.
2. The asset manager creates the maintenance window definition and relates it to the appropriate CIs.

Schedule definitions—blackout windows

The asset manager defines blackout windows. A blackout window is the time when a CI must not be brought down. For example, the server used by payroll might have a blackout window when paychecks are processed.

In an asset blackout schedule, when a CI is *available*, it is available for outages (for example, to perform maintenance). In the asset blackout schedule, when a CI is *unavailable*, it is unavailable for outages.

Figure 3-P: Schedule definitions—blackout windows

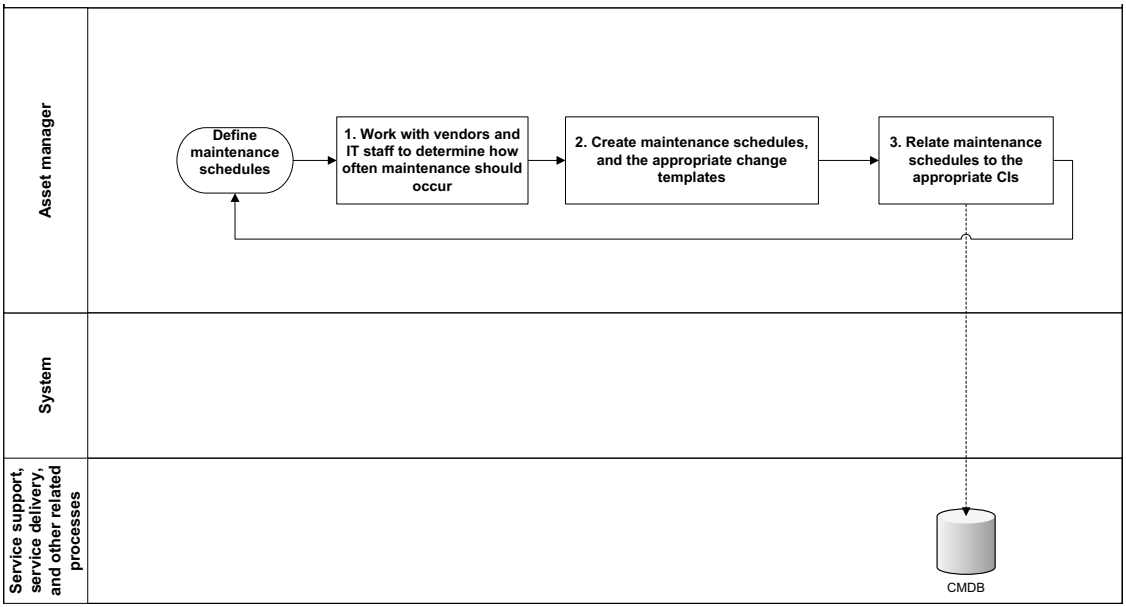


1. The asset manager works with business to determine when changes cannot occur to CIs or groups of CIs.
2. The asset manager creates a blackout window definition and relates it to the appropriate CIs.

Schedule definitions—maintenance schedules

The asset manager defines maintenance schedules. Maintenance schedules determine how often maintenance should occur.

Figure 3-Q: Schedule definitions—maintenance schedules



1 The asset manager works with vendors and IT staff to determine how often maintenance should occur.

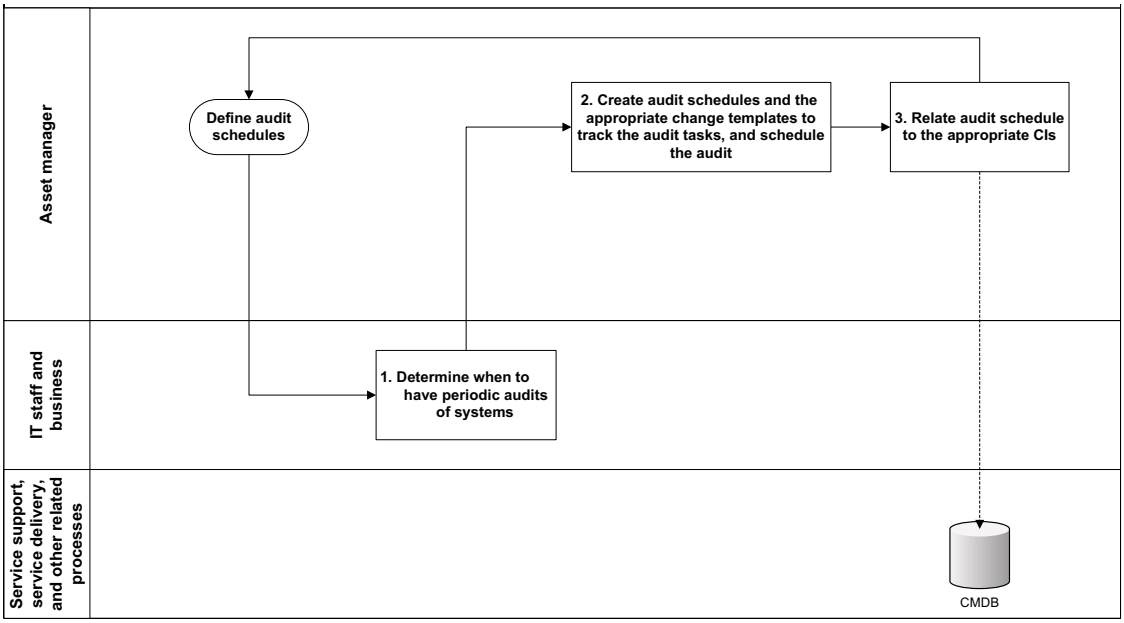
2 The asset manager creates maintenance schedules, and the appropriate change templates.

3 The asset manager relates the maintenance schedules to the appropriate CIs.

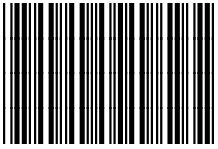
Schedule definitions—audit schedules

The asset manager, working together with IT staff and the business, defines audit schedules.

Figure 3-R: Schedule definitions—audit schedules



1. IT staff and the business determine when to have periodic audits of systems.
2. The asset manager creates audit schedules and the appropriate change templates to track the audit tasks, and schedules the audit.
3. The asset manger relates the audit schedule to the appropriate CIs.



66260