ITIL® ASSET AND CONFIGURATION MANAGEMENT

ITIL 4 Guide ›

IT services are typically made up of a bunch of individual components — things like servers, software and middleware, and unique configuration information.

In ITIL v3, Service Asset and Configuration Management (SACM) is about properly planning and managing (and reporting and auditing) the relationships and attributes of all of these components, across every service in your infrastructure.

In this article, we'll be exploring the activity of SACM as it functions in ITIL v3. This is part of our ITIL v3 Guide, which you can navigate using the right-hand menu. For the latest ITIL version, see our ITIL 4 Guide.

What is Service Asset and Configuration Management?

SACM is a combination of two important processes:

- **Asset management** which addresses the assets you use to deliver IT services.
- **Configuration management** which tracks the configurations of and relationships between the various components (configuration items or CIs) of your various IT services

Free Download ›

Free Download ›

According to ITIL, SACM is:

The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

This critical practice spans the entire service lifecycle. Nailing SACM is important to the health of both your individual services and your entire IT organization — and as such, it's often one of the first ITIL processes implemented in top IT organizations.

Goals of SACM

At its core, SACM is about ensuring that you are able to identify and control all assets across your infrastructure, and can manage their integrity through effective recording, reporting, and auditing.

More specifically, ITIL dictates that the objectives of SACM are to:

- Ensure that assets under the control of the IT organization are identified, controlled and properly cared for throughout their lifecycle.
- Identify, control, record, report, audit and verify services and other configuration items (CIs), including versions, baselines, constituent components, their attributes and relationships.
- Account for, manage and protect the integrity of CIs through the service lifecycle by working with change management to ensure that only authorized components are used and only authorized changes are made.
- Ensure the integrity of CIs and configurations required to control the services by establishing and maintaining an accurate and complete configuration management system (CMS).
- Maintain accurate configuration information on the historical, planned, and current state of services and other CIs.
- Support efficient and effective service management processes by providing accurate configuration information to enable people to make decisions at the right time — for example, to authorize changes and releases, or to resolve incidents and problems.

SACM definitions

Before we dive deeper, it's helpful to get a few definitions out of the way that you'll see regularly throughout this process and beyond. There are a ton of definitions, but we'll limit it to the most important ones for a basic functional understanding of the ITIL Asset and Configuration Management.

Configuration Management System (CMS)

A **Configuration Management System** is basically just a set of tools (like databases, files, etc.) that are used to gather, update, and analyze data about all of your configuration items and their relationships. A CMS may also include information about:

- Incidents
- Problems
- Known errors
- Changes
- Releases
- Sometimes even corporate data about employees, suppliers, locations and business units, customers, and users

This is different from a CMDB.

Configuration Management Database (CMDB)

A CMDB is a database that stores configuration records. One or more CMDB's may be part of the overarching CMS.

Configuration records

Config records describe your CIs by recording information about:

- Attributes, like name, location, version number, etc.
- Relationships among your CIs

Configuration items (CIs)

CIs are simply any component that needs to be managed in order to deliver an IT service. A server, a virtual server, or even the configuration of an application could be considered a CI, for example.

There are different types of CIs, including:

- **Service lifecycle CIs** such as business cases, service management plans, service lifecycle plans, service design package, release and change plans, and test plans, etc.
- **Organizational CIs** like the organization's business strategy, regulatory requirements that need to be managed to, etc.
- **External CIs** such as external customer requirements and agreements, releases from suppliers or sub-contractors, and external services.
- **Interface CIs** that are required to deliver the end-to-end service across a service provider interface (SPI), such as an escalation document that specifies how incidents will be transferred between two service providers.

Service assets

Service assets can be any resources or capabilities that contribute to the delivery of a service. Unlike CIs, which can be specifically managed by IT, service assets can't always. The knowledge of an IT worker, for example, is a service asset. The overall ability for a team to respond to an incident

or problem is a service asset.

SACM scope

If it's an asset that you use during the Service Lifecycle, it typically falls under the scope of SACM. Most things are fair game, including virtual assets, but there are some exceptions to the scope of SACM:

- Service assets that are not CIs are excluded from the scope. For example, the knowledge used by an experienced service desk agent to manage incidents.
- Assets that are not under the control of change management are excluded, such as information stored on a server.
- Non-IT assets in general are excluded. Everything else is fair game, including virtual assets.

In general, the scope of SACM includes management of the complete lifecycle of every CI — including interfaces to internal and external service providers where there are assets and configuration items that need to be controlled.

SACM benefits

Benefits of service asset and config management include:

- Better cost management of services
- Improved planning and delivery of changes and releases
- More efficient resolution of incidents and problems, meeting SLAs more frequently
- Less risk of non-compliance to important legal, regulatory, and procedural standards

Along the way, service asset and configuration management will interface with nearly all of your other IT process, including change management, financial management, incident and problem management, and more.

Key activities of SACM

There are six main activities in service asset and configuration management:

Planning

For each of the services you offer, ITIL suggests that you create a Service Management Plan — which is essentially just a document that addresses the critical components of a service before you implement it. It typically covers:

- The scope and objective of a service
- The activities and procedures (and even roles and people) required
- The relationship with other processes
- The tools and CIs also involved

Service Management Plans typically go into quite a bit more detail, though — outlining explicitly how the change management and configuration management processes will interface, how and when CI data will be audited, and much more.

Identifying

This is essentially creating a complete "inventory" of all the CI's in your infrastructure. In this activity, you are essentially recording every bit of data about your CIs that is necessary for effective operations — from the version of a piece of hardware or software to all the documentation, configurations, ownership details, etc.

To do so, ITIL recommends that you give all CIs **unique identifiers** (for example, numbers) and record all the relevant attributes of the CI (including the owner). Attributes you may want to capture include:

- The unique CI identifier and CI type. Every CI should have a unique identification number that makes it easily identifiable.
- The name and description of the CI
- Version numbers, since multiple versions of the same CI often exist
- Location and owner information, so you know where to find it
- Current status (ordered, in production, etc.)
- When necessary, supplier information, related documentation, etc.

Control

Here, ITIL recommends that all CIs follow a strict process for being added, changed, and removed from your CMS or CMDB. The goal is to ensure that changes of any kind don't occur without following your approved procedures for a wide variety of processes like license management, change management, version management, and even deployment.

Along the way, you will need to create your own policies and procedures for things like:

- **Controlling software licenses** to avoid noncompliance and prevent financial waste.
- **Controlling access** to facilities and systems.
- **Capturing the baseline of your assets and CIs before releases** to give you an accurate way to verify the success of actual deployments.

Status accounting and reporting

Throughout the lifecycle of every CI, ITIL encourages you to keep track of the complete status — including what changes have been proposed, the status of approved changes, etc.Being able to view and provide status reports gives you important insight into both the current and historical state of your CI's, and can even help you detect unauthorized CI's along the way.Reports typically include things like:

- An inventory of CIs and their baseline configurations
- An itemization of any unauthorized CIs
- Updates on recent changes or exceptions
- An itemization of hardware and software assets

Verifying and auditing

At any given time, you need assurance that your data is accurate on all of your CIs. Regular reviews and audits are essential, and ITIL recommends that you perform them to prevent discrepancies

between your actual environment and how it is documented.

In ITIL terminology:

- **Verification** is an ongoing activity, consistently ensuring that the CMDB accurately reflects all of your CIs.
- **Auditing** is a more formal, occasional deep dive to confirm not only that records are accurate, but that processes are being followed and standards (including SLAs, etc.) are being met.

Verifications and audits can be performed anytime, both randomly and according to a planned schedule. Tools are available to automate the process, too — comparing the configuration of designated servers with the master configuration you've recorded, for example. Audits are also often performed before major changes or releases are deployed, to avoid potential incidents or service disruptions.

Managing information

Ensuring the integrity of your configuration and asset data and systems is equally important. As part of the asset and configuration management process, you need to regularly back up the CMS, keep detailed records about archived and historical CI versions, and take appropriate measures to ensure data integrity across the entire lifecycle.

SACM best practices

To get the most from your SACM activities, follow these best practices:

1. Always ensure that changes to every configuration item are authorized by change management, and that all changes and updates also modify the relevant configuration records accordingly.
2. Ensure that you have the right checks and balances in place to prevent unauthorized personnel from moving hardware assets, or making changes to any assets or CIs. When this happens, the CMS becomes out of date — and it's important that your records stay accurate.
3. Stay vigilant about performing regular verifications and occasional audits, too. The goal is to prevent the accuracy of your configuration records, etc. from diminishing over time — and that can happen when you stop paying attention to the process and the results.

Additional resources

For more on this topic, explore the ITIL v3 Guide, with 20+ articles on the official ITIL methodology. For more information on ITSM in general, explore the BMC Service Management Blog.