INTRODUCTION TO CONFIGURATION MANAGEMENT

Enterprise IT assets are often deployed in a complex and hybrid mix of deployment architectures across on-site datacenters and cloud environments. These assets have configurations, or interface dependencies, between each other that must be identified, managed, and controlled to ensure that the IT environment behaves as required:

- Any change in configurations can dramatically impact the performance, security, and functionality of the code and the underlying IT assets.
- Infrastructure configured to run tests can be vastly different from the requirements of the production environment.

The task for IT Operations is to ensure that the configurations are managed correctly, following frameworks and guidelines such as ITIL®. In this article, we will explore the key concepts associated with configuration management, its components, and the activities involved.

What is configuration management?

Service Asset and Configuration Management (SACM) is an IT Service Management (ITSM) process that ensures assets, such as hardware, software, licenses, documentation, facilities, and people, are organized, configured, and administered so that you have accurate and reliable information about those assets when needed. Understanding the assets and the relationships among them reduces risk and supports other ITSM processes around change, incidents, and problem-solving.

Configuration management can also be described as activities associated with a technology platform that automates this process at scale.

A good example is DevOps environments where a mix of hybrid and multi-cloud services and assets are employed: companies use a Configuration Management System (CMS) to identify configuration states, control the changes, and audit the process for compliance and validation. A comprehensive CMS solution will ensure that the configurations are accurately identified, tracked, managed, and controlled across different SDLC stages, projects, and even the involved organizational departments.

Components of configuration management

Service assets and configuration management are closely associated and encompass all components, products, and services that must be managed from their inception to retirement.

IT professionals involved with Configuration Management will repeatedly come across the following key concepts:

- **Configuration model**: A tool that consolidates interactions between dependent components and service assets that must be managed and controlled. The model connects these components, evaluating infrastructure changes and causes of incidents.
- **Configuration item (CI)**: Any infrastructure or service component that requires management in order to enable an IT service. A CI can be a fundamental structural unit in a CMS that can be managed and modified independently of other components in the IT environment. Examples range from documents and models to hardware assets and software components.
- **Configuration records**: A set of records describing CI attributes and relationships.
- **Configuration management database (CMDB)**: A database that stores configuration records, including relationships between the configuration items.
- **Service asset**: Resources that enable the delivery of an IT service. These can include the services provided by third-party vendors or the overall capability of an organization to address IT and security incidents. Therefore, service assets are not necessarily manageable by the organization, but the information about their *state* can support critical decisions related to IT service delivery.
- **Definitive management library (DML):** A protected library containing authorized versions of configuration items as well as master copies of controlled software and documentation. The DML also defines capacity planning activities, security arrangements, and audit procedures.

The purpose of configuration management

Configuration management is intended to realize the following goals for IT projects, regardless of your ITSM framework:

- **Defining, identifying, and understanding configuration dependencies between assets.** Any configuration change has the potential to affect the service performance and security.
- **Maintaining accurate configuration information across the varied state of infrastructure assets.** Accurate information of the configuration states allows IT teams to maintain the IT environment in an optimal state for every individual phase of the SDLC lifecycle, such as development, test, production, and release.
- **Supporting informed decision making** such as change authorization, release management

and incident resolution, and other related service functions of an ITSM framework.
- **Controlling how configurations are updated and modified.** These controls encompass Infrastructure as a Code (IaaC) and Configuration as a Code (CaaC) practices adopted in a DevOps setting. Ensure that formal approvals are followed for releases into controlled environments.
- **Documenting configuration information and accounting for changes that may affect the integrity of CIs.** Audit the configuration management process to ensure that the necessary security and compliance protocols are followed.

IT configuration management examples

Configuration management is essential for system reliability, reduced downtime, and fast resolution of issues. A well-developed SACM makes it easier to track software, hardware, and network configurations and then make changes in a controlled and well-documented way. Configuration management is especially vital for critical changes, like system upgrades, responding to incidents, and going through a regulatory audit.

- **Network configuration management**: Describes how routers, firewalls, and switches are configured so that they are optimized for performance, reliability, and security, and minimize downtime.
- **Cloud environment management**: Uses configuration management tools to monitor and adjust settings of cloud resources to scale, maintain consistency, enable repeatable deployment, and stay in compliance in dynamic cloud environments.
- **Software version control**: Tracks and manages code changes and application configurations to make developer collaboration easier and to provide detailed change history for when rollbacks are needed. This results in fewer compatibility issues and reduced downtime, particularly during updates.
- **Database configuration**: Tracks and documents settings, database schema, and procedures with each version to maintain performance, availability, and a consistent environment. Configuration management in tracking and documenting ensures data integrity.

Configuration management process

To achieve these goals, incorporate these actions into your regular IT activities to support Continuous Improvement:

bmc

Configuration Management activities	
Management and planning	Document your configuration management plan: describe the level of configuration management applied to various service assets and components.
Configuration identification	Define and classify service assets and components to be managed across their whole service lifecycle. Describe the hierarchical relationships of CIs with associated documents, changes, incidents and the wider configuration structure in the IT environment.
Configuration control	Introduce policies and procedures to control software licensing, access and build control. Ensure compliance of data migration, asset distribution, and installations. Follow the protocols necessary to maintain a high quality and secure DML.
Status accounting and reporting	Track the progress and variation across changing states of CIs. When a CI moves through lifecycle phases, the CMS should record the status changes. The reports can include configuration states of each CI, including their baseline, modified, and deviated configurations.
Verification and audit	Perform reviews and audits to align the configuration states with documented baselines. Before introducing a change or release, verify the configuration information against specified requirements. You'll discover unregistered CIs during this audit phase, so you can apply necessary controls before including secure CIs in the DML.

ITSM and configuration management

ITSM is based on the idea that IT works as a service, with processes for designing, creating, and delivering those services, that can be managed from end-to-end and optimized for customer satisfaction and efficiency. Configuration management is a key part of ITSM.

IT Service Management

IT Service Management aligns the design, delivery, and management of IT services with the business needs of an organization, ultimately improving user and customer satisfaction. Configuration management provides accurate information about the IT environment, which makes other ITSM practices work more efficiently and with less risk. Configuration management supports incident management, change management, service request management, and problem management.

Configuration management supports ITSM processes

Configuration management activities are closely related to other ITSM domains. Specifically, it is related to change management, a process with which configurations are changed to support the removal, addition or modification of a service component that can affect the delivery of an IT service.

Other relevant service domains can include financial management, availability management, and incident and problem management, among others.

Additional resources

BMC Blogs offers a variety of beginner and advanced topics about IT service management, including configuration and asset management. For more information, consult our guide on ITSM, with 20+ related articles.

Ready for the only end-to-end ITSM and ITOM platform for your company? Explore BMC Helix.