WHAT IS A CONFIGURATION ITEM?

Two incidents caught my attention recently. The first was in New York City, where 14,000 parking meters rejected credit card payments due to an anti-fraud security setting that disabled the feature on January 1, 2020. Then Microsoft disclosed that over 250 million user analytics records were exposed on five ElasticSearch servers following a change to its security rules early in December 2019. They resolved the issue on the last day of the year.

Both scenarios were attributed to configuration errors, with Microsoft stating that "Misconfigurations are unfortunately a common error across the industry." Indeed, managing configurations is one of the more challenging activities in IT service management. So, what better way to look at configuration items than by defining what is it that we configure? In this article, we'll define CIs and look at real-world examples.

Defining configuration items

Let's look at how configuration items (CIs) are defined by some leading ITSM sources:

- ITIL® 4 defines a CI as any component that needs to be managed in order to deliver an IT service.
- ISO/IEC 20000:2018 says a CI is any element that needs to be controlled in order to deliver a service.
- CMMI SVC calls a CI an aggregation of work products that is designated for configuration

management and treated as a single entity in the configuration management process.
- Perhaps most broadly, SIAM says a configuration item includes anything used to deliver or support the services.

Based on these definitions, you might realize that there is no discernible difference between CIs and assets. However, it is important to note that while all CIs are assets, not all assets are CIs. Configuration items have an element of control required to deliver services, and this is not usually a preserve for all assets.

So, for example, knowledge or furniture can be classified as assets for your company. But they are not CIs, as they are not controlled for purposes of delivering services.

Examples of configuration items

CIs vary widely in complexity, size, and type, ranging from an entire service or system including all hardware, software, documentation, and support staff to a single software module or a minor hardware component. Here are common examples of CIs:

bmc

Configuration Items: Examples of common CIs	
Services	Email, printing, collaboration, presentation, data processing, user registration
Software	Applications, databases, virtual machines, containers, licenses
Hardware	Servers, routers, computers, switches, printers
Devices	Laptops, tablets, smartphones, monitors, keyboards, mice
Documents	Policies, governance, release notes, user guides, troubleshooting manuals
Locations	Offices, data centers, server rooms
Staff	Service desk agents, support specialists, developers

CIs may be grouped and managed together. For example, a set of components may be grouped into a single release.

Managing CIs

Managing CIs requires a systematic approach in order to prevent misconfiguration. Your approach should consider two functions:

- Collecting and maintaining accurate, organized CI records
- Regularly verifying and validating your CI information

Let's look at both activities in more detail.

Keep accurate, organized CI records

The first step in preventing misconfiguration is to collect and keep accurate and organized records of the CIs in your environment. Records of configuration items are usually held in configuration management systems or databases. Most ITSM solutions come with a CMDB, which is essential for correlating CI information with incidents, changes, requests, releases and deployments, plus supporting other practices such as information security and financial and systems audits.

While these solutions usually have myriad fields for each CI, at a bare minimum the ISO 20000 standards requires the following fields:

- Unique identifier
- Type
- Description
- Relationship with other CIs
- Status

Collecting and recording CI information sounds simple, but the practical application is something else. I paraphrase a quote from the VeriSM publication: Configuration management is referred to as the 'unicorn' of service management – everyone has heard of it, everyone knows what it is, but *no one* has seen it in real life!

Unless automated, diligently administered, and appreciated within your organization, chances are good that your staff views the act of recording, tracking, and correlating information on CIs as a laborious and low-value activity. The discipline required is no small matter, and it takes a significant amount of governance to make this happen. Some organizations choose to delegate the role to the service desk or other roles, but, in my opinion, the practice should be owned by system administrators working hand in hand with other stakeholders involved in the service delivery activities.

Best practice: Automate configuration management and include several stakeholders in its upkeep.

Verify and validate CI information regularly

Avoiding misconfiguration starts with configuration management, but it also requires administrators to regularly verify and validate the information stored in the organization's configuration management system.

Almost all organizations keep CI information in separate repositories and, as a result, getting a common view of this information is extremely challenging. Even though hosting all your applications on the cloud might provide easy visibility, the management of up-to-date information remains a significant hurdle when there are other pressing needs, such as incidents and projects.

Governance helps in getting people to understand the need to constantly check the reliability of your CI data. This governance should include capturing baseline data and comparing with snapshots, which also support easier troubleshooting and implementing and tracking changes.

Best practice: Establish CI governance for routine data checks, which trickle into easier troubleshooting and clearer change affects.

The necessary value of CIs

In determining the root causes of the Microsoft and New York City incidents, it is no surprise that both incidents could have been avoided if only someone took time to ensure that configurations were well validated and regularly reviewed at all levels.

Though configuration management may sound tedious, it is essential to successful and holistic ITSM. Other ITSM practices such as incident, problem, change, request, release, and deployment management can never be effective if configuration items are not properly recorded and the information shared visibly and accurately to all stakeholders. Understanding the value of CIs and the need to invest in CI management can go a long way in helping service providers meet the needs of customers and other stakeholders in more efficient and effective ways.