Configuration Management Best Practices

A Step-by-Step Guide

Configuration Management is at the core of effective service management. The quality of data within the Configuration Management Database (CMDB) affects the efficiency of the entire corporate Service Management strategy, as all processes utilize and feed into Configuration Management. As defined by ITIL, Configuration Management is more than a simple registry of physical assets; it includes documentation, Service Level Agreements, service catalogs, warranties, and knowledge. It enables the enterprise to manage the evolving relationships of those assets with customers, internal departments and locations, other organizations, and external suppliers.

Rules of the CMDB

Rule 1: Be in Control
Organizations must remain in control of Configuration Items and the ways they change. If control is lost, then the process is worthless.

Rule 2: Rely on Technology
Manual Configuration Management may prove to be impossible. You need to use technology to help discover, record, and maintain configuration information.

Rule 3: Discover the Chain Reaction
Configuration Management makes other things happen. Implementing Configuration Management by itself is a waste of time. Your Configuration Management program must enable your Change, Incident, Problem, and Release management programs if you want to see a return.

1) Build Variance Detection -- Configuration management must be able to efficiently supply CI build information, as detective controls are vital to change management and detected changes can examined for process problems, human errors, or security incidents that require immediate attention.
2) Inadequate information about the CI configuration can disrupt the change process, requiring extra time to analyze the CI and can result in incorrect planning that leads to availability problems, missed dates, and poor performance.
3) Data Mining for Problem Management -- Engineers investigating incidents can mine configuration records to look for corresponding incidents when certain CIs are used in a certain way
4) Enhance Ability to Rebuild -- In the event of a CI disaster, it is easier to rebuild if the final production build is known. If the final build exists as a drive image, the new hardware can be matched to the last known good build and the image can be restored. Unlike manual processes, recovery can be completed in minutes.
5) Assist with Budgeting -- Understanding the hardware and software involved in a given CI allows proper costing in the budget plan. Costing information is also important for ensuring the firm has adequate insurance. Tracking CIs allows IT to rapidly report what capital assets are in use, being decommissioned, or transferred to other departments or divisions.
6) Assist with Licensing -- Understanding what software is deployed allows management to track how many tools are in production and properly manage license counts. Firms want to have enough licenses to avoid legal disputes, but control spending by not having too many.

Tip: Couple with Change Management: In order to keep configuration items up-to-date, update the Configuration Management Database (CMDB) as part of every change. The configuration manager should only make modifications to items in the CMDB when an approved change is in place.
Configuration Management Serves all other ITIL processes

Configuration Management is tasked with capturing, keeping and providing up-to-date information about the IT infrastructure. Every IT organization has information about its infrastructure, particularly after completing major projects or when audit and impact analyses are done. Configuration Management aims to provide reliable details about the IT infrastructure. It holds the details of specific items in the infrastructure, what Configuration Management calls Configuration Items (CI’s). One of the most important characteristics of Configuration Management is how it relates these CI’s to one another. It is this relationship that is the key differentiator between the seldom implemented Configuration Management and the more common process of Asset Management. If IT organizations are to significantly improve services, a well run Configuration Management process is critical.
Configuration Management Best Practices

Implementation Steps

Step 1: Create a Plan
Implementing a Configuration Management program can be an arduous task, so it’s critical to set a realistic project timeline and to start with the basics. If you try to do too much, you’ll never get the program off the ground. Starting in a reasonable, limited fashion allows you to gain control in certain areas and build on established success thereafter.

Step 2: Establish a Repository
Organizations must have a repository for storing accurate configuration information.

Step 3: Develop a Process
Follow a defined process to populate the CMDB: Create a logical process such as, populate all physical infrastructure, create relationships for the physical infrastructure, add commercial off-the-shelf software, including relationships, then, populate business and custom applications.

Tip: Freeze changes before you populate your CMDB: Prior to populating the CMDB, set a policy to freeze all changes. Once you populate the items into the CMDB, control all future modifications through change management.

Step 4: Define the Right Configuration Items (CIs)
There are literally thousands of CIs that you could track, but trying to track them all would be a waste of your time and resources. Instead, look at each layer of your IT infrastructure (applications, operating systems, hardware, and services) to determine the most appropriate set of CIs and relationships to track and monitor.

Step 5: Slow Down
Beware of falling down the slippery slope of thinking Configuration Management and the CMDB are things that must be fully populated from the beginning. Take time to follow the simple steps of locating the sources of data, taking them under management control, and creating a system for knowing what is where and populating your CMDB as you go.

A Good Change Management Tool Should Include the Ability to Handle the Following:
1) Store all IT configuration information (software, hardware, equipment) in a database, and provide links and dependencies to ensure full understanding of impact prior to implementing a change
2) Enforce standardized Configuration Management methods and procedures
3) Changes and updates to CI’s are recorded, tracked and verified
4) Unauthorized and invalid changes are eliminated with process enforcement and approval cycles
5) Full reporting capabilities from the high-level down to the smallest details
6) Manage and report on Key Process Indicators (KPIs) such as accurate configuration data and linkages

www.techexcel.com