

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)

A VA Executive's Guide to Configuration Management

INTRODUCTION

This TS Note discusses Configuration Management (CM), which is not so much a technology as it is an important component of managing technologies. CM refers to a discipline for evaluating, coordinating, approving or disapproving, and implementing changes in artifacts that are used to construct and maintain software systems. Artifacts can mean a piece of hardware, software, or documentation. This note will discuss an overview of CM, its history, benefits, and its importance to the Department of Veterans Affairs (VA), and more specifically, how Technology Strategies (TS) is helping the agency define implement CM principles.

CM verifies that a system is performing as intended and that it's identified and documented in detail to support its projected life cycle. CM highlights the functional relationship between parts and systems for effectively controlling system change. Changes to the system are proposed, evaluated, and implemented using a standardized, systematic approach to ensure consistency. CM verifies that changes are carried out as prescribed and that documentation reflects the correct configuration. A complete CM includes provisions for storing, tracking, and updating all system information on a component, subsys-

tem, and system basis. Let's dive deeper into the history of CM and its purpose.

OVERVIEW AND PROCESS

Configuration Management (CM) was first introduced in the 1950s by the United States Department of Defense (DoD) as a technical management correction for hardware material items. In the 1960s, it became its own technical discipline when DoD developed the "480 series" for military standards. Since then, CM has developed further throughout military use and is now widely adopted by numerous organizations. Its concepts include: system engineering (SE), Information Technology Infrastructure Library (ITIL), product lifecycle management, application lifecycle management, and much more.

CM can simply be known as the practice of handling changes so that a system maintains its reliability over time. CM implements policies, procedures, techniques, and tools required to manage, evaluate, track, and maintain changes in an inventory system and documentation. For instance, during system development, CM allows project management to track requirements throughout the life cycle. As changes are made, they must be approved and documented to create an accurate record of the system status. The

Technology Strategies

Defining OI&T's
"To Be"
Technology
Vision



The TS office within OI&T's Architecture, Strategy & Design (ASD) interacts not only with the ASD pillar offices, but also with multiple stakeholders within OI&T and with strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for interagency operability.

core components of CM to keep in mind are: monitoring, discovery tools, domain specific configuration and change automation, software distribution, business intelligence, audit, and compliance.

CM DISCIPLINES

The CM process for both hardware and software configuration items comprises five disciplines. These are carried out as policies and procedures for establishing baselines and performing standard change management. These disciplines include:

- **CM Planning and Management:** A formal document and plan to guide the CM program that includes items such as: Personnel, Responsibilities and Resources, Training requirements, Configuration control, Audits and Reviews, etc.
- **Configuration Identification (CI):** Setting and maintaining baselines, which define the system or subsystem architecture, components, and any developments at any point in time; the basis by which changes are identified, documented, and tracked.
- **Configuration Control:** Evaluation of all change requests and change proposals, and their subsequent approval or disapproval.
- **Configuration Status Accounting:** Process of recording and reporting config-

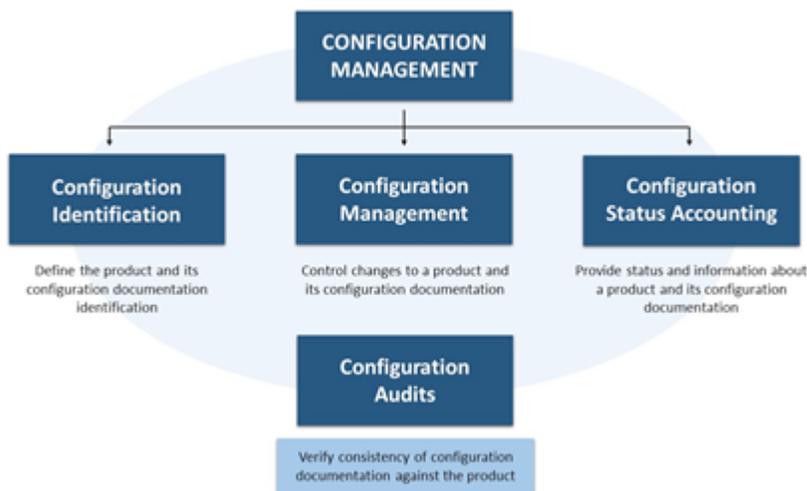


Figure 1: Configuration Management Process

A VA Executive's Guide to Configuration Management

Continued from Page 1

uration item descriptions (e.g., hardware, software, firmware, etc.) and all departures from the baseline during design and production.

- Configuration Verification and Audit: Review of hardware and software to assess compliance with established performance requirements, commercial and appropriate military standards. Audits verify system and subsystem configuration documentation complies with functional and physical performance characteristics before acceptance into an architectural baseline.

CM DATABASE (CMDB)

A CMDB is a database that contains all relevant information about the components of the information system used in an organization's information technology (IT) services and the relationship between these components. CMDBs provide an organized view of data and means of examining this data from different perspectives. It manages configuration items, and specifies, controls, and tracks these items and changes made to them in a systematic method. Think of a CMDB as a centralized repository to store all significant information on components in the IT environment.

ITIL specifications for CM include four major tasks of CM: identify CIs to be included in the CMDB; control data to ensure that it can be changed by authorized individuals only; maintain system status; and verify data to ensure that it is accurate.

Benefits of using a CMDB include:

- Ability to monitor and catch any unapproved changes to project plants, including why the changes were made
- Gather history to use for project audits and lessons learned
- Easily revert to a previous plan revision
- Compare between any points in time – between project phases or milestones

Challenges to using CMDB:

- Key product requirements are not being realized in final products
- Changes occur, but they're not consistently implemented
- Documentation does not describe actual conditions
- Changes are not being controlled and procedures are not being followed
- Problems are repetitive and costly

Another approach to CM is using a Configuration Management System (CMS), a software tool that provides support for configuration, change, and release management. It's the master system that controls one or more CMDBs. Therefore, CMDBs are not the only entity holding all information about all configuration items, but rather a collection of repositories that roll up data into the CMS. With that said, a CMS will be beneficial to businesses and even the VA.

CONFIGURATION MANAGEMENT, VA, AND THE IT VISION

There are several reasons why VA requires a solid CM strategy. Software licenses are not deployed in an enterprise-wide manner, resulting in overlaps and gaps. Therefore, VA needs to focus on synchronizing and integrating existing technologies to close any gaps in information security at a reduced total operating cost. A CMS will improve management of relationships between information systems, hardware, documentation, and configuration items, and will create a standardized reporting system to senior leadership. On top of this, it will minimize the impact of future incidents to the network and enforce enterprise-wide compliance with the Technical Reference Model (TRM). The VA "To Be" CM approach is to consolidate multiple repositories into a single federated database. Advantages to this include:

- Increased transparency and performance of the IT infrastructure
- Increased autonomy among different database structures
- Consolidated IT content into one powerful repository, for managing configuration and reporting to senior leadership
- Encouraged loosely coupled architecture to control VA CIs and IT Assets
- Track any changes to the CIs and IT Assets; provides a comprehensive view from a single access point

The Ruthless Reduction Task Force (RRTF) states in their System Divestiture Organization Design document that there is no single authoritative configuration management database. This impacts the ability to expeditiously identify all asset inventories resulting in decreased efficiencies and increased probability of excluding IT assets in the case of system divestiture.

Information Technology Service Management (ITSM) provides strategic guidance on the process established by VA to implement enterprise-wide IT asset management capabilities including configuration management of services in the IT infrastructure. According to the ASD Enterprise CMS White Paper, ITSM mandates that VA adopt a single, authoritative configuration management system. A reliable system provides organizations and agencies with a systematic process in order to monitor their IT environments, and the VA can benefit from this.

TS is currently working on an ITSM Enterprise Design Pattern with specific CM content. If you would like to contribute to or learn more about this Enterprise Design Pattern, please contact Jackie Meadows-Stokes.

If you have any questions about configuration management, don't hesitate to ask TS (askTS@va.gov) for assistance or more information.

Check out earlier TS Note editions [here](#).

(http://www.techstrategies.oit.va.gov/docs_ctsnotes.asp).