Chief Information Officer
Centers for Medicare & Medicaid Services

CMS Policy for
Configuration Management

April 2012

Document Number: CMS-CIO-POL-MGT01-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes the policy for Configuration Management (CM) of Information Technology (IT) assets of the Centers for Medicare & Medicaid Services (CMS) to include all automated systems, software applications and products, supporting hardware and software infrastructure (e.g., equipment, networks, and operating systems), and associated documentation, whether located at a CMS site or a site housing those assets on behalf of CMS.

2. BACKGROUND

CMS recognizes the necessity of managing its inventory of IT assets and changes to them in a disciplined manner to ensure the integrity and availability of these assets to support CMS' mission. As a result, CMS has tailored or customized the ISO/IEC 12207, *Software Life Cycle Processes,* standard to meet the specific needs of the Agency and is documented in the CMS Expedited Life Cycle (XLC) framework. The XLC follows the best practices used by both industry and government and requires the implementation of all appropriate security controls, including those related to Configuration Management, consistent with CMS Minimum Security Requirements (CMSR), FISMA, NIST requirements, standards and guidelines, other federal legislation, regulation, and executive orders..

Since its development by the United States Department of Defense in the 1950s, the concepts and practices of configuration management have been widely adopted by numerous management models such as Capability Maturity Model Integration (CMMI), ISO 9000, and COBIT.

The XLC framework establishes an environment in which CMS IT investments and projects consistently achieve successful outcomes that align with CMS' goals and objectives. Policies, processes, procedures, artifacts, reviews, and standards associated with configuration management are inherent in this framework.

3. CONFIGURATION MANAGEMENT OVERVIEW

Configuration Management (CM) is a discipline to ensure that the configuration of an item (and its components) is known and documented, and that all subsequent changes to it are controlled and tracked. The goals of using CM are to ensure the integrity of a product and to make its evolution more manageable. Effective CM imposes control over the activities that require the updating and using of multiple versions of project artifacts.

IEEE standard 729-1983 for Configuration Management and the Information Technology Infrastructure Library (ITIL) Framework both highlight four classic operational aspects of CM:

- **Identification:** An identification scheme is needed to reflect the structure of the product. This involves identifying the structure and kinds of components, making them unique and accessible in some form by giving each component a name, version identification, and configuration identification.

- **Control:** Control the release of a product and changes to it throughout the life cycle by having controls in place that ensure consistent software via the creation of a baseline product, an approval mechanism for changing baselines, and access control mechanisms that ensures changes are only made by authorized personnel/processes. This often involves implementing policies and processes to manage change both internally within the performing organization as well as change requests coming from external sources such as client requests and regulatory changes.
- **Status:** Record and report the status of components and change requests, and gathering vital statistics about the product.
- **Audit/Review:** Validate the completeness of a product and maintain consistency throughout the entire project life cycle to ensure that the product is maintained as a well-defined collection of components.

Keeping these definitions in mind, there are ten key elements to identifying and addressing the CM needs of a project. The first seven relate to preparation, planning, and performing the necessary work. The other three are the results of the previous seven.

- **Planning:** Identifying, resolving, and documenting in the CM plan the objectives of the CM initiative and related organizational relationships, tools, resources, internal and external dependencies, policies, procedures, federal regulations, etc.
- **Process:** Defining the actual CM process and what level of control will be enforced upon its implementation
- **People:** Identifying and defining all the various roles and responsibilities of those working on and impacted by the CM initiative
- **Culture:** Understanding the organizational culture as it exists before the implementation of CM and how the impact of incorporating CM tools, processes, and practices will impact that culture. Plan approaches to mitigate any potential issues
- **Product:** Determining what product(s) and part of product(s) will be placed under CM
- **Automation:** Deciding on the requirements for the functionality of an automated CM system
- **Management:** Resolving managerial decisions associated with the CM solution such as buying or building a CM solution

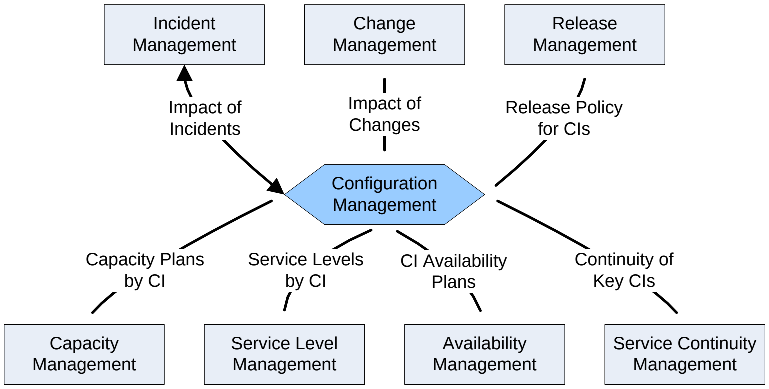
- **CM plan:** The actual document that summarizes the needs, planning, processes, procedures, policies, schedules, responsibilities, etc. defined to integrate a CM system within an organization
- **CM system:** The tool(s) chosen to assist in automating parts of the CM process. Choosing the most appropriate tool(s) for the performing organization requires extensive expertise in CM. In addition, tool review and approval by all appropriate authorizing individual(s) and/or department will be required prior to any selection. Often organizations have CM tools in place that are recognized as standards to be used by all projects.

- **CM adoption strategy:** The strategy implemented by an organization when adopting a CM process and/or system

CM is implemented to keep the inevitable changing of project artifacts under control by eliminating the confusion and errors that result from dealing with multiple versions of project artifacts. Successful CM requires well-defined policies, procedures, and standards that clearly define things such as:

- What CIs are currently under CM
- How artifacts enter and exit CM
- How CIs and other artifacts are named
- How CIs are allowed to change
- How different versions of CIs are tracked, made available, and can be used
- What CI information will be reported and how will CI records be maintained
- What CM tools are used to enforce CM

This and other relevant information, policies, and standards should be documented within a Configuration Management Plan (CMP). The CMP is used to document and inform project stakeholders about CM within the organization, what CM tools and processes will be used, and how they will be applied by the project. In addition, components of the CMP are also used to manage the implementation of the CM system.



Once implemented, every other process, directly or indirectly, interacts with the CM system. The ITIL Framework defines a number of process groups and how each group benefits from timely and accurate CM data and processes. This relationship is illustrated in the image to the right.

4. SCOPE

This policy applies to all IT activities and IT assets owned or controlled by CMS, including those of CMS’ agents, contractors or other business partners when acquired or supported by CMS funding. As such, this policy applies to all hardware, software, supporting infrastructure (e.g., equipment, networks, and operating systems), services, and associated documentation regardless of origin, nature, or location (e.g., contractor, in-house, development, operations, all hosting data centers, internal and external systems) unless otherwise specified.

5. OPERATIONAL POLICY

The CMS Configuration Management Program consists of a multi-layered structure comprised of policy, processes, procedures and standards, with each layer providing an increasing level of detail. The CM policy, processes, procedures and standards shall be followed unless specifically designated as optional or discretionary.

5.A. CM Planning & Management

All tasks necessary to implement CM principles and to conduct configuration activities shall be planned, coordinated, and managed throughout all lifecycle phases of a project, product, or automated system. The CM planning process shall be fully documented, and the documentation readily available to all levels of development, implementation, and operations management to formalize involvement and ensure continuity of CM practices.

5.B. Configuration Identification

Configuration identification is the process of identifying and documenting the functional and physical characteristics of items that are to be placed under configuration control. Configuration identification includes the selection of CIs, determination of the types of configuration documentation required for each CI, the assignment of unique identifiers to each CI and the technical documentation describing its configuration, and the establishment of configuration baselines. A hierarchical structure shall be established that identifies and summarizes the CIs comprising a given project, product, or automated system. Configuration identification information shall be maintained and readily available to all CMS decision makers.

5.C. Configuration Control / Change Management

Configuration control consists of the evaluation, coordination, approval or disapproval, and implementation of changes to CIs after formal establishment of their configuration identification. Effective configuration control depends on placing products under control and on establishing mechanisms for controlling changes to the products.

A systematic and measurable change process and procedures shall be implemented that is consistent with industry best practices and CMS' CM policy, CMSRs, and standards. The implemented change process and procedures shall ensure proposed changes are properly identified, prioritized, documented, coordinated, evaluated, and adjudicated. Approved changes shall be properly documented, implemented, verified and tracked to ensure incorporation in all applicable systems and/or products. Changes identified during ongoing maintenance of products/systems operating in production shall cycle forward into new business needs for appropriate analysis and consideration prior to modification of existing, or development of new, products/systems in response to requested changes.

Utilization of a Configuration (or Change) Control Board (CCB) is the CMS-preferred change control forum for establishing CM baselines and approving/disapproving subsequent changes to those baselines. A CCB may exist at the enterprise and/or project level, with an approved charter and operating procedures, as appropriate.

5.D. Configuration Status Accounting

Configuration status accounting focuses on recording and reporting information needed to maintain integrity and traceability of a controlled CI and its associated documentation throughout its life cycle. This includes monitoring the status of proposed changes and the implementation status of approved changes. Status accounting information includes developing and maintaining site configuration data and the incorporation of modification data on products and CIs.

Configuration status accounting information shall be developed and maintained for CIs in a systematic and disciplined manner in accordance with this policy, CMSRs, and CMS' CM standards, processes and procedures. This configuration information must be available for use by CMS decision makers over the life cycle of a project, product, or automated system and its identified CIs.

5.E. Configuration Audits

Configuration audits shall be performed to verify that a product's requirements have been met and that the product design meeting those requirements has been accurately documented before a product configuration is baselined or is migrated to the production environment. In addition, developmental and operational systems shall be periodically reconciled against their documentation to ensure consistency between a product and its current baseline documentation. Verification of the incorporation of modifications is a critical function of this activity. Periodic audits of software and hardware configuration baselines in the production environment shall be performed to ascertain that no unauthorized changes have been made without proper approval.

6. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

6.A. Chief Information Officer (CIO)

The CIO is responsible for the following activities:

- Providing leadership and direction regarding establishment, implementation, and administration of a viable CM Program for the CMS enterprise; and
- Assisting CMS' Business Owners/Partners, System Owners/Managers, and the Office of Information Services (OIS) in understanding their CM responsibilities and ensuring that they incorporate an acceptable level of configuration control into their projects, products, or automated systems.

- Developing, disseminating, and reviewing/updating within every three hundred sixty-five (365) days:
    - A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    - Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

6.B. Office of Information Services (OIS)

The OIS (or its identified Designee) is responsible for the following activities:

- Developing and implementing processes, procedures, and standards to ensure compliance with Section 4 above;
- Establishing a baseline configuration for each information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of a CMS information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of each information system is consistent with CMS' enterprise architecture.
- Establishing and documenting mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in CMSR CM-6 Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
    - Implementing the configuration settings;
    - Identifying, documenting, and approving exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
    - Monitoring and controlling changes to the configuration settings in accordance with organizational policies and procedures.
- Facilitating implementation of this policy, including providing appropriate training to ensure adherence to this policy;
- Monitoring adherence to this policy and reporting status to the CIO;
- Assisting System Developers, System Maintainers, and Project Owners/Managers with the development of CCB charters and operating procedures;
- Approving all established CCB charters and operating procedures;

- Coordinating and integrating activities of all CMS organizations working CM issues to optimize efficiency and eliminate redundant and/or contradictory efforts;
- Receiving, testing, and evaluating proposed mission unique or site unique CIs that may impact the CMS operational environment; and
- Performing configuration audits and following-up as necessary on identified corrective actions.
- Defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.
- Analyzing changes to each information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are authorized and audited.
- Developing, documenting, and maintaining an inventory of information system components that:
    - Accurately reflects the current information system;
    - Is consistent with the authorization boundary of each information system;
    - Is at the level of granularity deemed necessary for control, tracking and reporting;
    - Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
    - Is available for review and audit by designated organizational officials.

6.C. Business Owners, System Owners, and Project Managers

CMS' Business Owners/Partners, Project Owners/Managers, and System Owners/Managers are responsible for the following activities:

- Developing, documenting, and implementing a configuration management plan for each information system that:
    - Addresses roles, responsibilities, and configuration management processes and procedures;
    - Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
    - Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
- Establishing a CCB when appropriate, and ensuring that an approved charter and operating procedures exists for the established CCB;

- Ensuring that cost, schedule, risk, and performance aspects of change requests, problem reports, and engineering change proposals are known at the time of their consideration by the respective CCB;
- Participating in configuration audits; and
- Ensuring that a back-up and restore strategy is documented.

6.D. System Developers and System Maintainers

System Developers and System Maintainers are responsible for the following activities:

- Configuring the information system to provide only essential capabilities and specifically disabling, prohibiting, or restricting the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the Information System Description of the Security Plan (SP); all others will be disabled.
- Ensuring that CM activities are planned, coordinated, implemented, and managed for IT projects, products, or automated systems under their control in accordance with CMSRs and the CMS CM policy, processes, procedures, and standards established within the CMS Expedited Life Cycle (XLC);
- Contributing to the identification and control of CIs associated with their IT projects, products, or automated systems;
- Ensuring baseline configurations are adequately documented and maintained;
- Classifying and analyzing change requests and problem reports;
- Providing configuration status accounting reports to the appropriate personnel to report up-to-date status of baselined deliverables; and
- Participating in configuration audits.

6.E. Configuration (or Change) Control Boards

CCBs are responsible for the following activities:

- Ensuring that change requests, problem reports, engineering change proposals, or evolutionary builds are processed, evaluated, and adjudicated in a timely manner; and
- Evaluating the scope, applicability, and effect of proposed changes, focusing on the items that affect cost, schedules, or compliance with security or technical requirements, and providing approval/disapproval based on risk, defined strategic initiatives, program business objectives, and budgetary parameters.

7. APPLICABLE LAWS/GUIDANCE

The following laws and guidance are applicable to this policy:

- Acceptable Risk Safeguards (ARS) Appendix A: CMSR High Impact Level Data (CMS-CIO-STD-SEC01-1.0)
- Clinger-Cohen Act of 1996 (formerly called Information Technology Management Reform Act (ITMRA), Division E, National Defense Authorization Act for FY 1996 (P.L. 104-106), February 10, 1996
- CMS Expedited Life Cycle (XLC) Framework
- Federal Information Security Management Act of 2002 (P.L. 107-347)
- HHS IRM Guidelines for Capital Planning and Investment Control, HHS-IRM-2000-0001-GD, January 8, 2001, (especially Guideline A: Model Process, 3.4. Configuration Management and Guideline G: The Capability Maturity Model)
- IEEE standard 729-1983 for Configuration Management
- Information Technology Infrastructure Library (ITIL) Framework
- ISO/IEC 12207 Standard for Software Life Cycle Processes

8. EFFECTIVE DATES

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it, and remains in effect until officially superseded or cancelled by the CIO. This policy supersedes any previous policies issued regarding configuration management.

9. APPROVED

Signature: /s/ Date: ________________

Tony Trenkle
CMS Chief Information Officer and Director, Office of Information Services

10. RELATED DOCUMENTS

Document Name	Document Number and/or URL	Issuance Date

Table 1: Related Documents

11. GLOSSARY

Term	Definition
Automated System	A configuration of hardware and software infrastructure, applications, and associated documentation, either custom designed or commercial off-the-shelf (COTS) software, or combination thereof, that automates the activities of collecting and/or accessing data or information and performing logical computations in support of CMS' processes.
Baseline	(1) A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) A document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. (3) Any agreement or result designated and fixed at a given time, from which changes require justification and approval. (IEEE Std. 610-12-1990) A baseline is a configuration identification formally designated and applicable at a specific point in the life cycle of a configuration item.
Build	An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. (IEEE Std. 610-12-1990)

Term	Definition
Capability Maturity Model Integration (CMMI)	The CMMI® is a process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI® helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. The goal of the CMMI® is to improve usability of maturity models for software engineering and other disciplines, by integrating many different models into one framework. It was created by members of industry, government and the Carnegie Mellon Software Engineering Institute (SEI).
CMSR	CMS Minimum Security Requirements
COBIT	The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology governance.
Configuration	The functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product. (IEEE Std. 610-12-1990)
Configuration Audit	A functional configuration audit is conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional and allocated configuration identification, and that its operational and support documents are complete and satisfactory. A physical configuration audit is conducted to verify that a configuration item, as built, conforms to the technical documentation that defines it. (IEEE Std. 610-12-1990)
Configuration Control	An element of CM, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. (IEEE Std. 610-12-1990)
Configuration (or Change) Control Board (CCB)	A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. (IEEE Std. 610-12-1990)
CCB Charter	A document that defines the purpose, objectives, authority, membership, and responsibilities of an established CCB.
Configuration Identification	An element of CM, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. (IEEE Std. 610-12-1990)

Term	Definition
Configuration Item (CI)	An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration process. (IEEE Std. 610-12-1990)
Configuration Management (CM)	A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE Std. 610-12-1990)
Configuration Status Accounting	An element of CM, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes. (IEEE Std. 610-12-1990)
IT Project	A temporary endeavor undertaken to create a unique information technology product, service, or result (e.g., an automated system).
Product	A physical entity (e.g., a piece of hardware or software) or artifact (e.g., a document) that is created by someone or some process.