



UNITED STATES
DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT

MANUAL TRANSMITTAL SHEET

Release
1-1743

Date
6/19/2012

Subject:

H-1268-1 Information Technology Configuration Management Handbook

1. Explanation of Material Transmitted: This handbook implements the Configuration Management (CM) Manual – MS1268. CM is planning and managing the capacity and resources required to package, build, test, and deploy a release into production and establish the service specified in the customer and stakeholder requirements. CM aims to establish and maintain the integrity of all service assets and configurations, and provide efficient repeatable build and installation mechanisms that can be used to deploy changes to the test and production environments—and be rebuilt, if required to restore service.
2. Reports Required: None.
3. Material Superseded:
4. Filing Instructions: N/A.

REMOVE:

H-1268-1
Release 1-1680

(Total: 105 sheets)

INSERT:

H-1268-1

(Total: 17 sheets)

Lisa L. Jollay

Acting Assistant Director, Information
Resources Management
Bureau of Land Management

Bureau of Land Management
Configuration Management Handbook

BLM Handbook 1268-1

Table of Contents

Chapter 1. Overview	1-1
1.1 Purpose.....	1-1
1.2 Goals	1-1
1.3 Objectives	1-1
1.4 Value to the Mission	1-1
1.5 The Bureau of Land Management (BLM) Framework and Processes	1-2
A. Common Framework.....	1-2
1.6 Service Transition Processes.....	1-2
A. Change Management	1-2
B. Service Asset and Configuration Management.....	1-7
C. Release and Deployment Management.....	1-11
Appendix A: Roles.....	A-1
Appendix B: CM Process	A-3

Chapter 1. Overview

1.1 Purpose

This handbook implements the Configuration Management (CM) Manual – MS1268. As adopted from, and defined in the Information Technology Infrastructure Library® (ITIL) version 3, Configuration Management (CM) is planning and managing the capacity and resources required to package, build, test, and deploy a release into production and establish the service specified in the customer and stakeholder requirements. CM aims to establish and maintain the integrity of all service assets and configurations, and provide efficient repeatable build and installation mechanisms that can be used to deploy changes to the test and production environments—and be rebuilt, if required to restore service.

1.2 Goals

- a. Set customer expectations on how the performance and use of the new or changed Information Technology (IT) resource can be used to enable business change.
- b. Reduce variations in the predicted and actual performance of IT resources.
- c. Reduce errors and minimize risks associated with transitioning the new or changed IT resources into production.

1.3 Objectives

- a. Plan and manage the resources to successfully bring a new or changed IT resource into production within the predicted cost, quality, and time estimates.
- b. Ensure there are minimal, unpredicted impacts on the production IT resources, operations, and support organization.
- c. Increase customer, user, and support staff satisfaction with CM practices including deployment of the new or changed IT resource, communications, release documentation, training, and knowledge transfer.
- d. Increase proper use of the IT resources and associated applications and technology solutions.
- e. Provide clear and comprehensive plans that enable the customer and business change projects to align their activities accordingly.

1.4 Value to the Mission

- a. Improving the ability to adapt quickly to new requirements.
- b. Improving the success rate of changes and releases for the organization.
- c. Improving the predictions of service levels for new and changed IT resources.

- d. Improving confidence in the degree of compliance with mission and governance requirements during change.
- e. Reducing the variation of estimated and approved resource plans and budgets.
- f. Improving the productivity of business and customer staff through effective planning and the use of new and changed services.

1.5 The Bureau of Land Management (BLM) Framework and Processes

- a. **Common Framework.** In accordance with MS 1268, “Configuration Management,” ITIL v3 is designated as the underlying framework for BLM CM activities. The following framework and underlying procedures, processes, standards and guidelines are hereby defined:

Publications Background. The ITIL Core consists of five publications: Service Strategy; Service Design; Service Transition; Service Operation; and Continual Service Improvement. The BLM CM Process will utilize the Service Transition publication only until a comprehensive ITIL Service Strategy and Design is developed and implemented throughout BLM IT functions.

The Service Transition publication provides guidance for the development and improvement of capabilities for transitioning new and changed services into operations. The publication provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operations while controlling the risks of failure and disruption. The publication combines practices in release management, program management, and risk management and places them in the practical context of Service Management. It provides guidance on management, the complexity related to changes to services, and Service Management Processes, preventing undesired consequences while allowing for innovation. Guidance is provided on transferring the control of services between customers and service providers.

1.6 Service Transition Processes

Note: Transition Planning and Support, Service Validation and Testing, Evaluation, and Knowledge Management processes are incorporated in each of the four remaining individual processes outlined below.

- a. **Change Management.** The objective of the Change Management process is to ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. The purpose is to execute standardized methods and procedures for efficient and prompt handling of all changes; record changes in the Configuration Management System (CMS) and minimize mission risk.

- i. The process model includes: (a) the steps that should be taken to handle the change, including the handling of issues and unexpected events; (b) the chronological order these steps should be taken in, with any dependencies or co-processing defined; (c) responsibilities; (d) timescales and thresholds for completion of activities; and (e) escalation procedures and communication protocol.
- ii. CM activities include: (a) planning and controlling changes; (b) change and release scheduling; (c) communications; (d) change decision making and change authorization; (e) ensuring remediation plans exist; (f) measurement and control; (g) management reporting; (h) comprehension of change impact; and (i) continual service improvement.
- iii. Individual Change Activities:
 1. Create and record the Request For Change (RFC)
 2. Review RFC and change proposal
 3. Assess and evaluate the change
 - a. Establish the appropriate level of change authority.
 - b. Establish relevant areas of interest (i.e., who should be involved in the Change Advisory Board [CAB])
 - c. Assess and evaluate the business justification, impact, cost, benefits and risk of changes.
 - d. Request independent evaluation of a change; address the seven Rs of CM: (1) who **raised** the change; (2) what is the **reason** for the change?; (3) what is the **return** required from the change?; (4) what are the **risks** involved in the change?; (5) what **resources** are required to deliver the change?; (6) who is **responsible** for the build, test, and implementation of the change; (7) what is the **relationship** between this change and other changes?
 4. Authorize the change by: (1) obtaining authorization or rejection decision; and (2) communicating the decision with all stakeholders, in particular the initiator of the RFC.
 - a. Update plans as necessary.
 - b. Coordinate change implementation: (1) collate the change documentation, e.g., baselines and evaluation reports; (2) revise the change(s) and change documentation; (3) Close the change document when all actions are completed.

iv. Outline of ITIL General Procedures for Local Development as Appropriate:

1. Change authorization policies, rules and procedures.

- a. For raising an RFC, including preparation and submission of change proposal.
- b. How change requests are tracked and managed, i.e., change records.
- c. How change requests are impact assessed and evaluated promptly.
- d. Identifying dependencies and incompatibilities between changes.
- e. For verifying the implementation of a change.
- f. Overseeing and evaluating deliverables from change and release implementation.
- g. To review changes regularly to identify trends and improvements, e.g., in the success or failure of changes and releases.

v. Types of Changes:

Normal Change: (such as changes to Service Portfolios, Service Definitions, Project Changes, User Accesses, Operational Changes) need to follow the Normal Change Management process, and can be further categorized as changes which are Major, Minor or Significant in nature, and they need to be referred to the various levels of management for the final authorization.

Standard Change: when the approach has an accepted and established procedure that is pre-authorized by Change Management that has an accepted and established procedure to meet a specific change requirement.

Emergency Change: reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Changes intended to introduce immediately required business improvements are handled as normal changes, assessed as having the highest urgency.

vi. Change Documentation Elements:

- a. Unique Number
- b. Trigger (e.g., to purchase order, problem report number, error records, business need, legislation)

- c. Description of the Change
- d. Identity or item(s) to be changed—description of desired change
- e. Reason for Change, e.g., Business Case
- f. Effect of not implementing the change (business, technical, financial etc.)
- g. Configuration items and baseline versions to be changed.
- h. Contact and details of person proposing the change.
- i. Date and time that the change was proposed.
- j. Change category, e.g., minor, significant, major.
- k. Predicted time frame, resources, costs and quality of service.
- l. Change priority: Immediate (putting life at risk; causing a significant loss or revenue or ability to deliver important public services; immediate action required); High—severely affective some key users, or impacting on a large number of users; Medium—no severe impact, but rectification cannot be deferred until the next schedule release or upgrade; and Low—a change is justified and necessary, but can wait until the next schedule release or upgrade.
- m. Risk assessment and risk management plan
 - Risk Categorization (high impact, high probability; high impact, low probability; low impact, high probability; low impact, low probability)
- n. Back-out and remediation plan
- o. Impact assessment and evaluation—resources and capacity, cost, benefits.
- p. Decision and recommendations accompanying the decision.
- q. Authorization signature (could be electronic).
- r. Authorization time and date.
- s. Target baseline or release to incorporate change into.
- t. Target change plan(s) for change to be incorporated into.
- u. Scheduled implementation time (change window, release window or date and time).
- v. Location/reference to release/implementation plan.
- w. Details of change implementer
- x. Change implementation details (success/fail/remediation)
- y. Actual implementation date and time.

- z. Review date(s).
 - aa. Review results (including cross-reference to new RFC).
 - bb. Closure.
- vii. CM Tracking and Document Numbering:

The current file numbering system is designed to be stored in the EMC Documentum document management application. The numbering scheme matches the same numbering scheme that is used by the National Applications group. Each National, State, National Center, and the Washington Office will generate tracking numbers for CM documentation according to this numbering scheme. This document numbering scheme is designed to be able to separate National Applications, state and center baselines and the BLM national baselines. *Note: Hardware and software used in more than two states requires national baseline processing.* This scheme prevents duplication of numbers between offices. CM tracking numbers will be managed by the local Configuration Manager. The following CM tracking number represents this numbering scheme. Each field is separated by an underline (_) character.

SSSS_VVVV_AAAA_DDDD_v#.##_R#.#_(YYYY-MM-DD)

SSSS – State, Center or National Baseline

VVVV – Vendor Abbreviation

AAAA – Application Abbreviation

DDDD – Document Type

v#.# -- Version Number

R#.# -- Release Number

(YYYY-MM-DD) Document Date

SSSS State, Center or National Baseline Code

This is a two to four digit field which indicates on which baseline the document applies to State abbreviations (AK, CA, ID, etc), NIFC (Fire), NTC (National Training Center), NOC (National Operations Center). DIRM (National Baseline)

VVVV Vendor Abbreviation

This is the abbreviation of the vendor in the case of COTS applications or the government agency that created the application in the case of GOTS applications.

AAAA Application / Change Abbreviation

This is the abbreviation of the application or change.

DDDD Document Type

This is a two to four digit field that lists the abbreviation for the type of document that is being stored.

VDD Version Description Document

NCAB Change request for the National Change Advisory Board

TR Test Report

CR Change Request

ND Network Diagram

TSR Test Summary Report

HWS Hardware Specifications.

SWS Software Specifications.

v#.# Version Number

The version number is either assigned by the vendor in the case of Commercial-Off-The-Shelf (COTS), the government agency responsible for the application, in the case of Government-Off-The-Shelf (GOTS) or the next revision number in the case of CPO and configuration changes. The version number is blank for Enterprise Services Network (ESN) changes.

R#.# Release Number

The incremental number that enumerates the major and minor releases of a product. The number to the left of the decimal designates each major release of the application. The number to the right of the decimal designates a minor release. Before an application is released the release number will be filled in by #s.

(YYYY-MM-DD) Document Approval Date

The date of the document is shown in the year, month, and day format. The value for the date is determined when the document is approved. Test documents are dated when the document is reviewed and released, VDDs are dated when the last signer of the document has signed, NCAB documents are dated when the change request is either approved or denied.

- b. Service Asset and Configuration Management. The objective is to define and control the components of services and infrastructure and maintain accurate configuration information on the historical, planned, and current state of the services and infrastructure.

The purpose is to identify, control, record, report, audit, and verify IT resources, including versions, baselines, constituent components, their attributes, and relationships. Also, to execute standardized methods and procedures for efficient and prompt handling of all changes; record changes in the CMS; and optimize mission risk. Finally, to ensure the integrity of configurations by establishing and maintaining an accurate and complete CMS.

viii. The CM Baselines

The CM baselines represent a snapshot of all BLM approved IT assets at a particular moment in time. They are dynamic and are subject to change with each investment decision that leads to acquisition and deployment of an IT asset. According to the BLM's Investment Management Process investment decisions are made by IT Investment Boards, IT managers, program sponsors and other designated managerial officials.

CM Baselines are tools used to maintain a record of those approved IT assets. They may serve as instruments for decision-makers to forecast usage of IT assets, examine emerging technological needs, and offer an opportunity to consolidate maintenance renewals, acquire additional licenses or upgrade hardware to maximize savings. CM Baselines are maintained at the National, State, National Center and Project level. State, National Center, and Project level CM baselines should be similar to National Configuration Management (NCM) baselines ("National Baselines"). The BLM's National Baselines will be categorized in seven areas: As-Planned As-Released COTS and Applications, As-Planned As-Released Hardware, Software Product, and Hardware Product, Enterprise Services Network (ESN) Changes, Configuration Changes and Group Policy Orchestrator (GPO) Changes.

1. As-Planned, As-Released Software Baseline

The As-Planned, As-Released COTS and Applications Baseline provides an overview of approved existing and future applications. It lists proposed configurations and final configurations. It may be used to help management officials plan workloads based on projected release schedules. It may also be used to assist managers with planning for future hardware upgrades based on software releases and their correlating system requirements.

2. As-Planned, As-Released Hardware Baseline

The As-Planned, As-Released Hardware Baseline provides an overview of approved future and existing hardware products. It lists proposed configurations and final configurations. It may be

used to help management officials with refreshment planning. It may also be used to help management officials standardize on equipment to help reduce the price of support inherent with having multiple systems by multiple vendors.

3. Software Product Baseline

The Software Product Baseline provides a listing of all approved software by product name, vendor, release date, version number, contract number, system owner and sponsor. It also contains the number of licenses available in the Bureau. It may be used by management to make purchasing decisions.

4. Hardware Product Baseline

The Hardware Product Baseline provides a listing of all approved hardware by product name, vendor, release date, platform, and contract number. It may be used by management to make purchasing decisions.

ix. Configuration Boards

Boards or teams function to baseline documentation, validate, and verify the integrity of the information, and finalize application/software configurations prior to submitting IT assets for release. Board or team members are responsible for validating compliance with CM policy and procedures. Membership must include experienced CM, Data, IT Security, and Records personnel and subject matter experts.

BLM will use National, State, and National Center level configuration boards or teams to baseline final release of documentation and their associated application and hardware throughout their life cycle. This includes new software development activities and projects. For project level CM, project managers may use boards, teams, or perform the functions of the configuration board. In addition, project managers are expected to perform the following CM activities: configuration identification, configuration control, status accounting, audits and reviews. Project Managers must submit project documentation to Systems Engineering and Security for their review, requirements, and approval. Project managers must manage, track, and document changes to their applications during development, acceptance, unit, integration, and system testing prior to releasing their final documentation and software to the National, State, or National Center level board. Project managers are not authorized to release an IT asset to BLM without the appropriate National, State, or National Center board concurrence or approval.

Under the direction of the designated authority, the National Configuration Advisory Board (NCAB) reviews final release documentation for newly acquired IT assets or IT assets under the authority of the National Information Technology Investment Board (ITIB) to validate that the project complied with CM policy prior to releasing IT assets to the National Configuration Management (NCM) Baselines. The NCAB is a group of people that advises the Change Manager in the assessment, prioritization, and scheduling of changes. This board is made up of representatives from all areas within the IT service provider, the business, and subject matter experts. The board's primary role is to maintain the integrity of NCM baselines by ensuring that IT assets are tested, documented, and coordinated with IT Security, Data, Records, Architecture, and system owners prior to granting approval to release to the NCM baselines. For existing IT assets, the NCM staff oversees final release to the NCM baselines and reports status to the NCAB. State and National Center level boards under the direction of their appropriate management inherit the national level role; however, they may expand their board's authority to include managing changes to existing IT assets or integrating their local CM board within their local ITIB board. Configuration Managers will ensure that all National, State, or National Center boards have charters that describe their purpose, objectives and responsibilities. All chartered boards will have correlating operating procedures. On occasion, there may be a need to address high impact, Emergency Changes, which will necessitate a calling of a National Emergency Change Advisory Board (ECAB). The ECAB is a subset of the NCAB, who make decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.

x. Testing Facilities

The BLM will use testing facilities and testers to document, conduct, and report test results on BLM's software and hardware IT assets. Testing must be conducted at BLM designated testing facilities, provided that they can meet the required test environment criteria. Although the National Test Lab facility (NTL) is the primary testing facility for national applications, NCM will use other BLM testing facilities as necessary to help with validation and release of national applications. NCM, working with the National Operations Center (NOC) Division of Information Resources Management (DIRM), will oversee the routing and scheduling of national applications to those facilities. Testing of National, State, and National Center Level Applications may also be performed by approved off-site contractors when needed to fulfill the CM testing requirements. NCM will maintain a listing of those facilities approved to test national

applications on their web site. State and National Center Configuration Managers are also required to maintain a listing of their approved testing facilities. Project managers must declare where testing will be conducted and identify those who will perform the testing in their draft master test plan. Moreover, all testing must be conducted at BLM NCM approved testing facilities.

Although testing may be done at approved testing facilities, all distributions and testing of national software and hardware will be coordinated through the NCM and NOC/DIRM staff. NCM uses an electronic mail box at :

BLM_NATIONAL_CONFIGURATION_MANAGEMENT@blm.gov to serve as a central repository for receiving CM documentation. The electronic mail box is monitored during core business hours by the NCM staff. State and National Center offices are encouraged to set up a similar electronic mail box for receiving State and National Center specific CM documentation and for distributing software and hardware.

c. Release and Deployment Management

- i. The goal of Release and Deployment Management is to deploy releases into production and establish effective use of the service in order to deliver value to the customer and be able to handover to service operations.
- ii. The purpose is to:
 1. Define and agree on release and deployment plans with customers and stakeholders.
 2. Ensure that each release package consists of a set of related assets and service components that are compatible with each other.
 3. Ensure that the integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the CMS.
 4. Ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate.
 5. Ensure that organization and stakeholder change is managed during the release and deployment activities.
 6. Record and manage deviations, risks, issues related to the new or changed service and take necessary corrective action.

7. Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities.
8. Ensure that skills and knowledge are transferred to effectively and efficiently deliver, support and maintain the service according to required warranties and service levels.

iii. There are three release types:

1. Major Releases: normally containing large areas of new functionality, some of which may eliminate temporary fixes to problems. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.
2. Minor Releases: normally containing small enhancements and fixes, some of which may already have been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
3. Emergency Releases: normally containing the corrections to a small number of known errors or sometimes an enhancement to meet a high priority business requirement.

Appendix A: Roles

Change Manager

- The Change Manager authorizes and documents all changes in the IT Infrastructure and its components (Configuration Items), in order to maintain a minimum amount of interruptive effects upon the running operation.
- In the case of further-reaching changes, he involves the Change Advisory Board (CAB).

Change Advisory Board (CAB)

- A group of people that advises the Change Manager in the Assessment, prioritization and scheduling of Changes.
- This board is usually made up of representatives from all areas within the IT Service Provider, the Business, and Third Parties such as Suppliers.

Emergency Change Advisory Board (ECAB)

- A sub-set of the CAB who makes decisions about high impact Emergency Changes.
- Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.

Project Manager

- The Project Manager is responsible for planning and coordinating the resources to deploy a major Release within the predicted cost, time and quality estimates.

Application Developer

- The Application Developer is responsible for making available applications and systems which provide the required functionality for IT services.
- This includes the development and maintenance of custom applications as well as the customization of products from software vendors.

Release Manager

- The Release Manager is responsible for planning, scheduling and controlling the movement of Releases to test and live environments. Their primary objective is to ensure that the integrity of the live environment is protected and that the correct components are released.

Configuration Manager

- The Configuration Manager is responsible for maintaining information about Configuration Items required to deliver IT services.
- To this end, they maintain a logical model, containing the components of the IT infrastructure (CIs) and their associations.

Knowledge Manager

- The Knowledge Manager ensures that the IT organization is able to gather, analyze, store and share knowledge and information.
- His primary goal is to improve efficiency by reducing the need to rediscover knowledge.

Test Manager

- The Test Manager ensures that deployed Releases and the resulting services meet customer expectations, and verifies that IT operations are able to support the new service.

Appendix B: CM Process

