Configuration Management Plan

FSA Systems

Revision: 1.1

Date: July 2016

United States Department of Agriculture
1400 Independence Ave., SW
Washington, DC 20250

Template Release October 2014

Document Information

Owner Details	
Name	Darren Ash, Chief Information Officer
Contact Number	202-720-5320
E-mail Address	Darren.Ash@wdc.usda.gov

Document Revision and History

Revision	Date	Author	Comments
1.0	November 2, 2015	Lois Thomson	Created CMP using OCIO October 2014 template.
1.1	July 11, 2016	Lois Thomson	Updated with assistance from Kendall Kukowski.

Distribution List

Name	Title	Agency/Office	Contact Information
	Chief Information Officer; Deputies-Chief Information Officer; Application Development Center (ADC), Architecture & Management Center (AMC) and Operations & Testing Center (OTC) directors; Program Management Office (PMO) chief, ADC applications architect; ADC office and group chiefs	Farm Service Agency	

Configuration Management Plan Authorization

We have carefully assessed the Configuration Management Plan for the FSA Systems. This document has been completed in accordance with the requirements of the USDA System Development Methodology.

MANAGEMENT CERTIFICATION

☑ The document is accepted.

JEFFERY
WAGNE
R

Digitally signed by JEFFERY WAGNER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=JEFFERY WAGNER, 0.9.2342.19200300.100.1.1=12001000333690
Date: 2016.07.11 12:56:36 -05'00'

Chief Information Security Officer   Date

GERALD
PATTILL
O

Digitally signed by GERALD PATTILLO
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=GERALD PATTILLO, 0.9.2342.19200300.100.1.1=12001001776814
Date: 2016.07.12 11:06:52 -05'00'

Director Architecture and Management Center   Date

Table of Contents

1 Introduction

Configuration management (CM) is the ongoing process of identifying and managing changes to deliverables and other work products. The configuration management plan (CMP) is developed to define, document, control, implement, account for, and audit changes to the various components of this project. The CMP provides information on the requirements and procedures necessary for CM activities and establishes the methodology for configuration identification and control of releases and changes to configuration items. It also describes the process for maintaining status accounting and verifying the completeness and correctness of configuration items throughout the system life cycle.

1.1 Background/Purpose

The Federal Information Security Management Act (FISMA) requires agencies to establish “minimally acceptable system configuration requirements” within their information security program, and the National Institute of Science and Technology Special Publication (NIST SP) 800-53, Rev. 4 defines a set of security controls which support this requirement.

The purpose of this document is to elaborate on the application of these security controls and provide guidelines for managing the configuration of the information system architecture and associated components for secure processing, storing, and transmitting of information in the information environment. Security configuration management provides an important function for establishing and maintaining secure information system configurations, and provides support for managing risks in information systems. This document describes the organizational framework, roles and responsibilities, general practices and activities, and artifacts necessary to guide the configuration management of information technology (IT) systems and capabilities within USDA.

The FSA Systems CMP is being established to control the maintenance of FSA Systems, using approved best practices approaches to tracking all change requests.

This CMP is consistent with, and directly applicable to, the USDA System Development Life Cycle (SDLC). This CMP establishes the configuration management activities that will be performed during the development and implementation phases of FSA Systems.

Configuration management supports the overall change management efforts, and deals primarily with creating and maintaining a logical model of the IT infrastructure and services by identifying, controlling, maintaining and verifying all relevant versions of configuration items (CI) in the infrastructure.

1.2 System Overview/CMP Scope

All systems developed or managed and funded in support of FSA programs are covered by this CMP. These include system, subsystems, and general support systems (GSS).

These systems are hosted on multiple GSSs, e.g., National Information Technology Center (NITC) mid-range, NITC mainframe, and National Finance Center, etc.

This CMP will be loaded on the Cyber Security Assessment and Management (CSAM) tool Status and Archive page and linked to Appendix Q at the FSA Program level. The unique system mission, data flow, system architecture, system administration and management activities may be found in individual system security plans.

1.3 Points of Contact

The points of contact for the unique systems and subsystems are listed on the “Roles” page for each specific JIRA project.

1.4 Applicable Policies, Standards, Procedures, and References

References used in the preparation of this document include:

•Configuration Management (CM), USDA DR 3520-002, August 12, 2014

•Security Assessment and Authorization (A&A), USDA DR 3540-003, August 12, 2014

•FSA Change Management Process Definition

2 Configuration Management Program

2.1 Configuration Control Board

The Change Control Board (CCB) is a system decision-making body that must approve all functional change requests before they can be implemented.

2.1.1 Structure

In FSA the CCB is a group typically consisting of two or more individuals that have the collective responsibility and authority to review and approve functional change requests to an information system.

At the minimum, a CCB must consist of a Configuration Management Authority (CMA)/Business Sponsor and a Configuration Control Authority (CCA)/IT Sponsor. Security responsibilities are left to the CCA/IT Sponsor.

By establishment of a CCB, the board approves and implements the FSA Systems Configuration Management Plan that is in accordance with the FSA Change Management Process Definition. This is available at the following Uniform Resource Locator (URL). http://www.fsa.usda.gov/FSA/sdlcapp?area=home&subject=ccm&topic=landing

NOTE: The FSA Systems Inventory CCB is separate and different than the System CCB. If CCB is used without a qualifier in this document it is referring to the System CCB, not the FSA Systems Inventory CCB.

2.1.2 Configuration Management Authority (CMA)/Business Sponsor

Every IT system is developed and implemented in response to a business need or as a solution to an operational problem. Business sponsors define requirements based on their operational needs and ensure that operational user requirements are properly identified, documented, approved, and implemented for all systems under development or being operationally maintained by their organizations.

The Business Sponsor or their designated representative authorizes changes to business requirements. The Business Sponsor represents business interests.

2.1.3 Configuration Control Authority (CCA)/IT Sponsor

Control of design solutions to meet the needs of operational user requirements rests with the CCA/IT Sponsor. The IT Sponsor, e.g., application development chief, technical review board, etc., or their designated representative must authorize changes to non-business requirements. The IT Sponsor represents technical interests.

2.1.4 Configuration Management Specialist (CMS)

The individuals operating as the Configuration Management Specialist (CMS) are critical to the successful operation of a configuration management process. Together they are responsible for ensuring that all elements of the change management process are followed and documentation is kept under their physical control.

Responsibilities:

- Implement the applicable organizational CM program and CM requirement baselines for all agency/site IT systems;
- Establish and maintain a change request CR tracking database based upon the CCB;
- Develop and publish the organization’s CM plan and operating procedures;
- Develop and review CCB roles, as required;
- Act as secretary to the applicable organizational CCB by preparing and distributing its agendas and minutes; recording status of CRs effected by CCB deliberations and preparing project change authorizations for CCB approved CRs if meetings are held;
- Produce and distribute periodic database, individual system, or product CR status reports if meetings are held;
- Support developer functional configuration audits (FCA) and physical configuration audits (PCA);
- Coordinate CRs with individuals responsible for implementation of approved changes (gate keeping); and
- Resolve all CR problems to promptly mitigate system/product impact.

At FSA the role of the CMS may be filled by an individual responsible for ensuring all change requests steps were documented as completed or separate individuals responsible for ensuring that prior change request steps were documented as completed.

2.1.5 Security Representative (ISSO/ISSPM)

Configuration management is more than looking at the functionality/operation of the system. It must include the security aspects of system operation and changes to the system that may change those security aspects. For this reason, the security representative is critical to the proper operation of the change management process.

Responsibilities:

- Review and evaluate changes to ensure the integrity of the system.
- Ensure mitigation of security risks.
- Review change processes to ensure that the modified configuration maintains its certification and accreditation status.
- Review and evaluate changes to ensure that proposed changes are in accordance with USDA and FSA security policy and guidance as well as applicable Federal laws, directives, policies, regulations, standards, and guidance.
- Advise appropriate security organizations on security status of configuration changes.
- Conduct Application Release Impact Assessment (ARIA) Security Impact Analysis that acknowledges the change has been reviewed relative to security issues.

For projects that do not have a security representative assigned, the FSA Chief Information Security Officer (CISO) designates the Configuration Control Authority/ IT Sponsor to represent security interests on the CCB.

2.1.6 Configuration Control Board Membership

Key change management roles are identified on the “Roles” page in JIRA.

2.2 Configuration Management Processes and Tools

2.2.1 Change Analysis

The change should be analyzed from each corner of the classic tradeoff triangle: How will the change affect the system’s schedule, cost, and features? It should also be analyzed from the point of view of each organization affected: How will it affect development, customer satisfaction/usability, documentation, customer support, and quality assurance? If the feature request is not worth the time it takes to analyze it, then it is not worth the time it will take to implement it, and the CCB should reject the proposed change.

The role of FSA CCBs is to analyze each proposed functional change required for CCB approval.

2.2.2 Triage

In addition to analyzing each change, the CCB has to accept or disapprove each one. Some organizations refer to this part of the CCB’s job as “triage,” a term from emergency medicine that refers to the activity of sorting injured people into groups so that the people who will most benefit from medical treatment receive it first. In the operation of a CCB, triage means allocating a scarce resource, and that there is not enough of the resource to go around. That is true in software development. There will never be enough time or money to add every feature that everyone wants. Triage also means that some people will not receive aid even though they desperately need it. In software, some changes that seem as though they are desperately needed will not make it into the next release of the software. Some features will not be implemented, and some low-priority defects will not be corrected. Finally, triage also means that something is life-critical. And when prioritizing change requests on a rapid-development system, the CCB is definitely performing a job that is critical to the life of system.

FSA CCBs make the critical decisions to proceed or not for those requests for changes that require CCB approval.

2.2.3 Bundling

The CCB also has the ability to group together small changes so that developers can handle them in bundles. A series of small uncoordinated changes can be extremely costly in the late stages of a project. Each one requires the overhead of a code review, documentation update, testing, checking files in and out of version control, and so on. It is much more efficient to develop small changes in groups rather than one at a time.

2.2.4 Configuration Management Tools

FSA uses JIRA, Subversion, and Nexus for library control, configuration inventory and change history, and status reporting.

2.2.5 Configuration Management Library

A configuration management library is a repository of all documentation concerning a specific phase of system development. It may help to provide traceability for the system from initial design through roll-out and production.

FSA has several configuration libraries for the software it develops: policy, change request/requirements, and release to production. They are outlined below with the related URLs.

Policy:

Information Security Program Policies

https://sharepoint.apps.fsa.usda.net/iso/public/Wiki%20Pages/ISPP.aspx

FSA Change Management Process Definition and System Development Life Cycle (SDLC)/Information Bulletins

http://www.fsa.usda.gov/FSA/sdlcapp?area=home&subject=ccm&topic=landing

Change requests/requirements:

JIRA

https://wiki.dev.fsa.usda.gov/display/FSADEV/Change+Management+%28CM%29+Landing+Page

https://wiki.dev.fsa.usda.gov/display/FSADEV/Change+Management+Process+-+FSA+Work+Tracker+in+JIRA

Release to production:

ARIA Security Impact Analysis

https://wiki.dev.fsa.usda.gov/pages/viewpage.action?pageId=18158056

2.3 Configuration Item Retention, Archiving, Storage, and Disposal

Configuration items are the products that are to be placed under configuration control. The FSA configuration items include applications, databases, and the general support systems. These products include the following items:

- Management documentation describing the processes used to develop or manage the development of the system,
- Technical documentation or baselines describing the system,
- Software components (computer programs, operating systems and support tools);
- Data and database components (files and records that exist apart from software, which access the contents of a database)

FSA retains records of configuration-controlled changes with JIRA. JIRA records are retained at a minimum of two years.

3 Configuration Management Activities

Configuration control is the systematic evaluation, coordination, approval or rejecting, and implementation of all proposed changes in the configuration of a configuration item after formal establishment of its baseline. Procedures must be established to ensure that changes are accomplished in an organized manner with traceability and accountability so that project CM requirements are properly implemented. Requested changes to software, hardware, data, networks, or documentation are formally reviewed and approved or denied in order to allow evaluation of the effect of the change on security, performance, interfaces, acceptability, completeness, and documentation.

3.1 Configuration Identification

This section describes how requests for change or problem reports are initiated, processed, and completed. It also outlines configuration management's role in life cycle reviews and audits, which are both formal mechanisms for establishing and reviewing project baselines.

3.1.1 Types of Configuration Items (CI)

FSA identifies that the system, databases, and general support systems are the configuration items.

3.1.2 Identification Criteria

The definition of a Configuration Item (according to the Release Tracker documentation and ITIL V3) is “any component that needs to be managed in order to deliver an IT service”. For Release Tracker, CIs only exist within the context of a Release Package, and the impacted system(s) is identified within that Release Package.

3.2 Configuration Baselining

A baseline is a collection of information describing the technical characteristics of each CI. Baselines serve as technical control points in the life cycle for the evaluation of proposed changes to these technical characteristics. The baseline and the approved changes or modifications provide a current description of the system.

The various baselines are:

Functional Baseline

The functional baseline, sometimes called the requirements baseline, is the main product of the define system phase and is managed in accordance with the functional requirements document and the data requirements document.

Design Baseline

The design baseline reflects activities performed during the design system phase. Its major component is a system/subsystem specification that defines the overall system design in terms of its subsystems, the allocation of requirements to subsystems and interfaces between subsystems and external systems. The user acceptance evaluation criteria component of this baseline is defined in the Verification, Validation, and Test Plan. The user acceptance evaluation criteria are not a separate document, but are a major element of the design baseline.

Development Baseline

The development baseline, generated during the build system phase, defines the detailed structure of the system being implemented. The development baseline’s major components are the generation of the computer programs (code) and the database. Other components include training, users, operations, and maintenance documentation.

Product Baseline

The product baseline is established during the evaluate system phase. The product baseline’s major component is the end system product as built by the developers. This includes the following:

- Software
- Design and specification documentation
- Manuals (user, operations, maintenance, etc.)
- Installation and conversion procedures

The product baseline is established after successful completion of the FCA,PCA, and associated system products and audit results presented at the evaluate system review. This baseline incorporates all changes needed to resolve problems detected during system acceptance and release testing, and any discrepancies identified between the system, its requirements, and design documentation.

Operational Baseline

The operational baseline is the primary baseline for a system/application in the operational phase of its life cycle. It originates from the product baseline and continues to evolve over time as the application undergoes updates and upgrades.

Baseline Tracking

FSA documents the system baselines that comprise the configuration of the system in the production request system, e.g., Nexus, Subversion, JIRA, etc.

3.3 Configuration Change Control

Refer to FSA Change Management Process Definition.

3.4 Configuration Management Monitoring

The change management process is monitored by internal and external reviewers multiple times annually in support of FISMA assessments, A-123 reviews, and Financial Statement audits. During reaccreditation the process is assessed by the security test and evaluation team.

A sample of change artifacts, e. g., Change Requests, Test Release Transmittals, ARIA Security Impact Analysis, and testing evidence, is used to verify that the change control process is in place and operating effectively.

3.4.1 Change/Problem Resolution Tracking

Issues identified during reviews of the configuration management process will be monitored through resolution. Informal methods are approved for use, however, formal methods up to and including creating Plans of Action and Milestones may be requested by management.

3.4.2 Measurements

The following measurements are used to determine the status of control implementation and effectiveness for CM activities and processes.

- Control weakness
- Control deficiencies (management letter recommendation)
- Significant deficiencies
- Material weaknesses

3.4.3 Configuration Status Accounting

All CM activities are recorded, stored, and reported by the configuration status accounting (CSA) function. The CSA function is a discipline that provides managers with feedback to determine whether decisions of the CCB are being implemented as directed. As approved changes are executed, the CSA function records and files data concerning the appropriately modified software, hardware, and documentation. The CSA function is responsible for identifying and issuing the most current approved versions of the CM-controlled items to project participants.

The status of changes is tracked. Change requests are recorded according to the current FSA Change Management Process Definition. Any changes that are approved and implemented are tracked in the production request system, e. g., JIRA, etc., and available for ad hoc reports. Artifacts that identify changes implemented are kept by FSA for the life of the production request system and according to record retention requirements thereafter.

The current FSA Change Management Process Definition provides steps to assure that the software meets the design intent, the requirements are satisfied, and the tests are performed in accordance with test plans.

3.4.4 Release Management

Generally, release management is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which will function as intended when introduced into the existing infrastructure. Quality control during the development and implementation of new hardware and software is also the responsibility of release management. This guarantees that all software meets the demands of the business processes. The goals of release management are:

- Plan the rollout of software;
- Design and implement procedures for the distribution and installation of changes to IT systems;
- Effectively communicate and manage expectations of the customer during the planning and rollout of new releases; and,
- Control the distribution and installation of changes to IT systems.

The focus of release management is the protection of the live environment and its services through the use of formal procedures and checks.

FSA-developed software releases to production are managed by the Information Processing and User Support Office (IPUSO.)

FSA notifies the support agencies that manage the hardware if new software requires upgrades of hardware.

3.5 Configuration Management Reporting

The FSA Information Security Program Policies, Configuration Management & Maintenance Policy outlines policy for system configuration. This may be found at the following URL. https://sharepoint.apps.fsa.usda.net/iso/public/Wiki%20Pages/ISPP.aspx

The baseline configuration of the system is reviewed: a) at least annually during the annual review of system security plan and annual assessments; b) when vulnerabilities with the current configuration are discovered; c) as a part of the security risk analysis conducted prior to implementation of any changes to the system.

3.5.1 Configuration Audits

Formal configuration audits are conducted at certain predetermined points as specified in the project plan. The purpose of the audit is to certify that the design, development, and integration meet the system’s technical requirement, that they are accurately documented, and that they do not include unauthorized changes. With complex administrative systems, informal audits should be performed to minimize the impact on project schedules and identify deficiencies as soon as possible. Deficiencies noted during the informal audit, as well as recommendations for any corrective actions, are made available for CCB review during the configuration audit. Configuration audits validate compliance of development requirements by comparing the functioning system to its technical documentation.

3.5.1.1 Informal Audits

Informal auditing is part of the standard SDLC process and is performed during integration testing, regression testing, and certification testing. Deficiencies founded during informal audits are reviewed and corrective action is taken accordingly.

3.5.1.2 Formal Audits

Formal configuration audits are conducted at certain predetermined points as specified. The purpose of the audit is to certify that the design, development, and integration meet the system's technical requirement; that they are accurately documented; and that they do not include unauthorized changes. Formal audits are done as part of the annual A-123 audit, the annual FISMA assessment, and the annual OIG financial statement audit.

4 Training

This section describes CM training for all project personnel.

FSA provides on-the-job training regarding configuration controls during the change management process. Roles and responsibilities are reviewed with the following groups.

- Development teams across FSA
- Change control boards across FSA and the business sponsors
- Testing and Certification Office (TCO) staff
- Production staff (IPUSO)
- Information Security Office (ISO) staff

Configuration management courses are available in AGLearn.

Information for on-the-job change management training is available at the SDLC FSA Configuration and Change Management Program at the following URL.
http://www.fsa.usda.gov/FSA/sdlcapp?area=home&subject=ccm&topic=landing

It includes the following information.

- FSA Change Management Plan Process Definition - defines the CM procedures that should be followed.
- FSA Change Management Compliance Checklist - a one page checklist to guide through the process of becoming compliant with the Change Management Plan Process Definition.
- JIRA CCB Implementation Guide - contains specific details regarding the change management process and the use of JIRA to manage the change control board.

Information for accessing JIRA may be found at the following URL.
https://wiki.dev.fsa.usda.gov/display/FSADEV/New+Process+for+Requesting+JIRA+Access?src=search

Information for HP Application Lifecycle Management (ALM) may be found at the following URLs.
https://sharepoint.apps.fsa.usda.net/otc/TCO/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fotc%2FTCO%2FShared%20Documents%2FHP%20QC%20Implementation%

20Strategy&FolderCTID=0x01200067604DB3E73E7B44AC72CB1A4AEFEE57&View={B43E4186-8484-4A62-AE1C-44D7F63BBF6A}
and
https://sharepoint.apps.fsa.usda.net/otc/TCO/Lists/HP%20QC%20FAQs/HPQCFAQS.aspx

TCO standard operating procedures may be found at the following URL.
https://wiki.dev.fsa.usda.gov/display/TCOT/TCO+SOPs

FSA Information Security Program Policies, Configuration Management & Maintenance Policy may be found at the following URL.
https://sharepoint.apps.fsa.usda.net/iso/public/Wiki%20Pages/ISPP.aspx

Appendix A. JIRA Change Request

The JIRA change request may be found at the following URL.

https://issues.dev.fsa.usda.gov/secure/CreateIssue!default.jspa