



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

2.125.1

OCTOBER 31, 2022

EFFECTIVE DATE

(10-31-2022)

PURPOSE

(1) This transmits revised IRM 2.125.1 Change Management Policy.

MATERIAL CHANGES

(1) Revised to satisfy the IRM internal control requirements.

EFFECT ON OTHER DOCUMENTS

IRM 2.125.1 dated September 19, 2018 is superseded.

AUDIENCE

The Change Management Policy is applicable to all Information Technology (IT) organizations, contractors, and other stakeholders having responsibility for change, management, oversight, and successful day-to-day operations of the IRS IT enterprise hardware, software, and services.

Nancy Sieger
Chief Information Officer

2.125.1

Change Management Policy

Table of Contents

2.125.1.1 Program Scope and Objectives

2.125.1.1.1 Background

2.125.1.1.2 Authority

2.125.1.1.3 Responsibilities

2.125.1.1.4 Program and Management Review

2.125.1.1.5 Program Controls

2.125.1.1.5.1 Controls

2.125.1.1.5.2 Metrics

2.125.1.1.6 Terms

2.125.1.1.7 Acronyms

2.125.1.1.8 Related Resources

2.125.1.2 Purpose

2.125.1.3 Scope

2.125.1.4 Mandates

2.125.1.1
(10-31-2022)
Program Scope and Objectives

- (1) **Purpose.** This document describes the formal Information Technology (IT) policy for implementing the requirements of the Change Management (ChM) process. It provides the purpose, scope, authority, and mandates for institutionalizing this process. The objective of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control the IT infrastructure to minimize the impact of any related incidents upon the service. All changes must be recorded and managed in a controlled way. The scope of Change Management covers changes to all configuration items (CIs) across the whole service lifecycle.
- (2) **Audience.** The Change Management policy is applicable to all IT organizations, contractors, and other stakeholders having responsibility for change, management, oversight, and successful day-to-day operations of the IRS IT enterprise hardware, software, and services.
- (3) **Policy Owner.** Demand Management & Project Governance (DMPG) Division, within Enterprise Operations (EOps) - Information Technology (IT).
- (4) **Program Owner.** Governance & Resource Management Branch (GRMB), within DMPG - EOps - IT.
- (5) **Primary Stakeholders.** IT organizations having responsibility for establishing an internal or local Change Management process and/or managing and controlling their IT system and/or system components are stakeholders in the IT Change Management process.
- (6) **Contact Information.** To recommend changes or to make any suggestions to this IRM section, email the IT ChM PMO: *it.chm.pmo@irs.gov*

2.125.1.1.1
(10-31-2022)
Background

- (1) This IRM establishes the IT Change Management process tailored from industry best practices and standards to support the system and operational requirements of the IRS.
- (2) This IRM enables the IT Change Management process to meet certain industry, federal, and regulatory requirements.

2.125.1.1.2
(10-31-2022)
Authority

- (1) IRM 1.2.1.3 *Policy Statements for Information Technology Activities*
- (2) Office of Management and Budget (OMB) *Circular A-130, "Managing Information as a Strategic Resource"*
- (3) Federal Information Security Modernization Act (FISMA) of 2014 (*Public Law 113-283, 44 USC 3554*)

2.125.1.1.3
(10-31-2022)
Responsibilities

- (1) The Director, Demand Management & Project Governance, is the Process Owner accountable for the IT Change Management process and providing resources for maintenance and support.
- (2) The Chief, Governance & Resource Management, is the Process Manager responsible for the IT Change Management Program Management Office (ChM PMO) under the Change & Configuration Management (CCMS) Section.
- (3) The IT ChM PMO is responsible for:
 - a. Developing and maintaining the IT Change Management policy and process for Infrastructure Change Management.

- b. Training and coaching Process Practitioners assigned to perform their roles defined in the IT Change Management process.
- c. Communicating and socializing the IT Change Management process throughout the process community and other key stakeholders.
- d. Improving the IT Change Management process through process and operational metrics, process assessments and audits, and process reviews and evaluations.

2.125.1.1.4
(10-31-2022)

**Program and
Management Review**

- (1) The IT ChM PMO shall manage and evaluate the process based on the following guiding principles:
- a. **Process Management.** The Change Management process will have a single Process Owner and a separate Process Manager, responsible for implementation and ensuring adherence to the process. The process will be reviewed regularly to ensure that it continues to support the business requirements of the enterprise. Process metrics will be focused on providing relevant information as opposed to merely presenting raw data.
 - b. **People.** Roles and responsibilities for the process must be clearly defined and appropriately staffed with people having the required skills and training. The mission, goals, scope and importance of the process must be clearly and regularly communicated by upper management to the staff and business customers of IT. All IT staff (direct and indirect users of the process) shall be trained at the appropriate level to enable them to support the process. It is imperative that people working in, supporting or interacting with the process in any manner understand what they are supposed to do. Without that understanding, Change Management will not be successful.
 - c. **Process.** Modifications to the Change Management process must be approved by the Process Owner. The design of the process must include appropriate interfaces with other processes to facilitate data sharing, escalation and workflow. The process must be capable of providing data to support real-time requirements as well as historical/trending data for overall process improvement initiatives. The process must be fully documented, published and accessible to the various stakeholders of the process. The process will be reviewed on a periodic basis to ensure it continues to support organizational goals and objectives (continuous improvement). The process must include Inputs, Outputs, Controls, Metrics, Activities, Tasks, Roles and Responsibilities, Tool and Data requirements along with documented process flows. The process will be kept straight forward, rational, and easy to understand. The process must meet operational and business requirements.
 - d. **Technology and Tools** All tools selected must conform to the enterprise architectural standards and direction. Existing in-house tools and technology will be used wherever possible, new tools will only be entertained if they satisfy a business need that cannot be met by current in-house tools. The selection of supporting tools must be process driven and based on the requirements of the business. Selected tools must provide ease of deployment, customization and use. Automated workflow, notification and escalation will be deployed wherever possible to minimize delays, ensure consistency, reduce manual intervention and ensure appropriate parties are made aware of issues requiring their attention. Technology and tools should be used to augment the process capabilities, not become an end themselves.

2.125.1.1.5
(10-31-2022)

Program Controls

- (1) Program controls are driven by the policies and guiding principles on how the process will operate.

2.125.1.1.5.1
(10-31-2022)

Controls

- (1) Controls provide direction over the operation of processes and define constraints or boundaries within which the process must operate.

Name	Description
Policies	Policies and criteria for the inclusion of a component and its attributes in the configuration management system..
Scope	Applicable to any change that might affect the IT systems, infrastructure, and services in the IT environment. This should also include changes to all architectures, applications, software, tools and documentation, as well as changes to all configuration items across the whole service lifecycle.
Management Reports	The frequency and distribution for regularly produced management reports.

2.125.1.1.5.2
(10-31-2022)

Metrics

- (1) Metrics are used for the quantitative and periodic assessment of a process. They should be associated with targets that are set based on specific business objectives. Metrics provide information related to the goals and objectives of a process and are used to take corrective action when desired results are not being achieved and can be used to drive continual improvement of process effectiveness and efficiency.
- (2) Management will regularly set targets for process performance, gather quantifiable data related to different functions of the Change Management process, and review that data to make informed decisions and take appropriate corrective action, if necessary. All measurements will have a defined data dictionary, map to the organizational strategic goals, and be documented in a Process Measurement Plan.
- (3) Enterprise and local Change Management processes, including Change Management tool owners, must produce metrics and measurement reports to measure the effectiveness and efficiency of the Change Management process.

2.125.1.1.6
(10-31-2022)

Terms

- (1) Process Owner. The ChM Process Owner is the single point of contact for the process at the enterprise level and is accountable for the overall quality of the process, ensuring that the process is performed as documented and is meeting its objectives.
- (2) Process Manager. The ChM Process Manager supports the ChM Process Owner and is responsible for the operational management of the process.
- (3) Process Practitioner. The ChM Process Practitioner are those assigned a role in the Change Management process that carry out its core activities.

- (4) **Policy.** Outlines a set of plans or courses of action that are intended to influence and determine decisions or actions of a process. Policies provide an element of governance over the process that provides alignment to business vision, mission, and goals.
- (5) **Process.** A set of linked activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon goal in a measurable manner.
- (6) **Objective.** Process objectives describe material outcomes that are produced or achieved by the process.
- (7) **Control.** Represents the policies and guiding principles on how the process will operate and define the constraints or boundaries within which the process must operate.
- (8) **Metric.** Defines quantitative and qualitative measures to track the performance of a process.
- (9) **Role.** Assigned to perform specific tasks within the process and its responsibilities are confined to the specific process. Roles do not imply any functional standing within the hierarchy of an organization. For example, the Process Manager role does not imply the role is associated with or fulfilled by someone with a functional management responsibilities within the organization.
- (10) **Configuration Item.** A collection and combination of hardware, software, and documentation that is used to deliver a product or service.
- (11) **Request for Change.** A formal proposal submitted by a stakeholder in the organization to alter a configuration item.

2.125.1.1.7
(10-31-2022)

Acronyms

- (1) This table lists commonly used acronyms and their definitions.

Acronym	Definition
CCMS	Change & Configuration Management
ChM	Change Management
ChM PMO	Change Management Program Management Office
CI	Configuration Item
DMPG	Demand Management & Project Governance
GRMB	Governance Resource & Management Branch
IT	Information Technology
RfC	Request for Change

2.125.1.1.8
(09-19-2018)

Related Resources

- (1) The following list the primary sources of guidance associated with the Change Management process.
 - IRM 2.125.2 *Change Management Process*
 - IRM 2.150.1 *Configuration Management Policy*
 - IRM 2.150.2 *Configuration Management Process*
 - IRM 2.22.1 *Unified Work Request (UWR) Process*
 - IRM 10.8.1 *Information Technology (IT) Security, Policy and Guidance*

2.125.1.2
(10-31-2022)

Purpose

- (1) The purpose of this Policy is to establish formal requirements to manage changes to IT systems, infrastructure, and services, ensure that a consistent and systematic approach is used for implementing changes, and control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. This includes establishing an IT-wide Change Management Program and to provide responsibilities, compliance requirements, and overall principles for the Change Management process to support information technology management across the IT organization.

2.125.1.3
(10-31-2022)

Scope

- (1) This Policy is applicable to any change that might affect the IT systems, infrastructure, and services in the IT environment. This should also include changes to all architectures, applications, software, tools, and documentation, as well as changes to all configuration items across the whole service lifecycle.

2.125.1.4
(10-31-2022)

Mandates

- (1) **All Changes to Configuration Items (CIs) will be registered.** To maintain accurate information and status of CIs, any proposed change to CIs supporting any IRS system, e.g., Production, Development, Test, Disaster Recovery, etc., will be recorded as a Request for Change (RfC) or Change Request (CR) in the approved Change Management system.
- (2) **All Changes must be approved prior to implementation.** All changes to CIs supporting any IRS system, e.g., Production, Development, Test, Disaster Recovery, etc., must be approved prior to their implementation.
- (3) **All Changes must be deployed in an approved window.** All changes shall be scheduled for deployment in an approved window, and can only be deployed outside that window if there is an accompanying Priority 1 or Priority 2 Incident Ticket that justifies the exception.
- (4) **Risk, Technical, Security, and Business Impact Assessment.** All changes will be assessed for risk and categorized based on risk. All RfCs must include an assessment of the risk and business impact of the change, as well as applicable technical and security assessments of the planned work. Changes impacting the forecast business results, documented in a work request, business case, or equivalent justification will be presented to the appropriate IT Executive Steering Committee (ESC) or Governance Board (if low risk and or low cost) for acceptance of the impact prior to approval of the RfC. This ensures a comprehensive review of proposed changes before they are authorized and approved for release into production.
- (5) **Review of Unsuccessful Changes and Incidents Caused by Change.** When changes are implemented, the success or failure of the implementation must be recorded on the RfC. Changes considered not successful include changes not implemented as planned; changes backed out, all or in part;

changes not implemented per schedule; and changes causing incidents. These unsuccessful changes will be reviewed by Change Management staff to determine the cause of the failure and plan remediation actions for the future.