



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

2.5.1

MAY 9, 2024

EFFECTIVE DATE

(05-09-2024)

PURPOSE

- (1) This transmits revised IRM 2.5.1, Systems Development.

MATERIAL CHANGES

- (1) Signature, Changed Chief Information Officer (CIO) from Nancy Sieger to Rajiv Uppal.
- (2) Effect on Other Documents, Changed the date from “December 15, 2021” to “October 07, 2022”
- (3) Changed the word “Agency” to “IRS” throughout this IRM.
- (4) IRM 2.5.1.1(3), Removed the word **Application Development** in front of CIO, because it was incorrect.
- (5) IRM 2.5.1.1.1(1), Removed Nancy Sieger.
- (6) IRM 2.5.1.1.1(1) Added new IRMs: (e) IRM 2.5.6, (f) IRM 2.5.8, (g) IRM 2.5.9 and Information Technology (a- j).
- (7) IRM 2.5.1.4.1.1, Removed the note for Interim Guidance because IRM 2.5.14 was not replaced with IRM 2.107.1.
- (8) IRM 2.5.1.4.13, Changed “Application” to “Software” Development to in the title.
- (9) Exhibit 2.5.1-3, Removed IRM 2.100.2 because it was obsoleted; added OneSDLC because it is new.

EFFECT ON OTHER DOCUMENTS

IRM 2.5.1, dated June 06, 2022 is superseded.

AUDIENCE

The audience intended for this transmittal applies to all IRS executives, Information technology (IT) managers at all levels, IT government and contractors. This includes personnel responsible for engineering, developing, testing, and maintaining IRS software systems identified in the IRS Enterprise Architecture.

Rajiv Uppal
Chief Information Officer

2.5.1
Systems Development

Table of Contents

- 2.5.1.1 Program Scope and Objectives
 - 2.5.1.1.1 Background
 - 2.5.1.1.2 Authority
 - 2.5.1.1.3 Roles and Responsibilities
 - 2.5.1.1.4 Program Management and Review
 - 2.5.1.1.5 Program Controls
 - 2.5.1.1.6 Acronyms/Definitions/Terms
 - 2.5.1.1.7 Resources
- 2.5.1.2 System Development Quality Assurance (QA)
 - 2.5.1.2.1 Configuration Controls
 - 2.5.1.2.1.1 Configuration Control Board
 - 2.5.1.2.1.2 Government Sponsor, Configuration Control Board (CCB)
 - 2.5.1.2.1.3 Chairperson, Configuration Control Board (CCB)
 - 2.5.1.2.2 Work Requests
- 2.5.1.3 Configuration Management (CM)
 - 2.5.1.3.1 Change Management (ChM)
 - 2.5.1.3.1.1 Organizational Change Management (OCM) Model
 - 2.5.1.3.2 Proposing a Change
 - 2.5.1.3.3 Requesting a Work Request
- 2.5.1.4 Directives
 - 2.5.1.4.1 System Development Quality Assurance (QA) Best Practices
 - 2.5.1.4.1.1 Audit Process Control
 - 2.5.1.4.2 Coordinate Change and Maintenance of System Change Control
 - 2.5.1.4.3 Coordinate Change of Software
 - 2.5.1.4.4 Curtail Software Defects
 - 2.5.1.4.5 Define System Configuration Controls
 - 2.5.1.4.6 Engineer Software Products
 - 2.5.1.4.7 Integrate Engineering and Managerial Activities
 - 2.5.1.4.8 Improve Processes and Maintain Process Assets
 - 2.5.1.4.9 Manage Requirements
 - 2.5.1.4.10 Manage Software Configurations
 - 2.5.1.4.11 Manage Software Contracts
 - 2.5.1.4.12 Plan Applications Development Projects
 - 2.5.1.4.13 Track and Oversee System Development and Software Development Projects
 - 2.5.1.4.14 Define/Plan Organizational Process Training

Exhibits

- 2.5.1-1 Terms and Definitions
- 2.5.1-2 Roles By Organizational Unit
- 2.5.1-3 Directives and Supporting Internal Revenue Manuals
- 2.5.1-4 Acronyms and Definitions

2.5.1.1
(05-09-2024)
Program Scope and Objectives

- (1) **Purpose:** This Internal Revenue Manual (IRM) and the other manuals that constitute IRM 2.5.1 Information Technology, Systems Development establishes the directives, procedures, standards, and other controls intended for the Government to:
 - a. Ensure the IRS's software systems are, in an efficient and effective manner, engineered, developed, and maintained.
 - b. Improve the IRS's capability to engineer, develop, and maintain software systems.
 - c. Improve the IRS's capability to transition from the current enterprise architecture to the target enterprise architecture.
- (2) **Audience:** This IRM 2.5.1 is the baseline guidance for all IRMs under IRM 2.5, and applies to all IRS executives, senior leadership, Information technology (IT) managers at all levels, IT government and contractors. Also included are all personnel responsible for: engineering, software development, computer programming, analytics, database administration, system administration, or maintaining IRS software systems identified in the Enterprise Architecture. This engineering, development, and maintenance include services performed by both government employees and contractors.
- (3) **Policy Owner:** Chief Information Officer (CIO)
- (4) **Program Owner:** Director, Technical Integration Organization (TIO)
- (5) **Primary Stakeholders:**
 - a. IRS IT managers and executives
 - b. Computer programmers - government and contractors
 - c. Quality Assurance (QA) managers and QA staff - government and contractors
 - d. Engineers - government and contractors
 - e. Software Developers - government and contractors
 - f. System Administrators - government and contractors
 - g. Database Administrators - government and contractors
 - h. Data Analyst - government and contractors

2.5.1.1.1
(06-06-2022)
Background

- (1) According to **GAO-21-524T** "Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems" as of April 2021, under the Modernizing Government Technology Act of 2017, the Technology Management Fund Board approved a portion of \$89M to the IRS as part of 11 IT modernization projects across seven agencies. This action allowed the IRS to continue mitigating existing and future legacy operational and security risks while moving to modernized solutions such as cloud computing as a continuous process.
- (2) Concluding on **GAO-21-524T** during January 20, 2022, the Chief Information Officer (CIO) signed Interim Guidance (IG) "IT-02-1121-0010" for IRM 2.16.1. The purpose of this IG is to initiate the "IT Decommissioning Policy" for providing guidance to ensure all Modernization Program/Project leads identify and own the decommissioning process of associated legacy system(s), product(s) and/or services(s) affiliated with the IRS IT Modernization plan.
- (3) In response to Government Accountability Office **GAO-18-298**" Information Technology (IT): IRS Needs to Address Significant Risks to Tax Processing-Investments Performance and Risks", June 2018 report provided to Congress-

sional Committees. IRS IT recognized the importance of continuously improving the performance of IRS Major IT Investments. IT IRS organizations' Mainframe systems, using legacy programming languages: Common Business Oriented Language (COBOL), Assembler Language Code (ALC), Java programming; etc., IRS Application Development (AD) has established Risk Management strategies and guidance to identify, analyze, mitigate, and monitor risks and issues for system development standards.

2.5.1.1.2
(06-06-2022)
Authority

- (1) Treasury Directive 85-1, Department of the Treasury Information Technology (IT) Security Program
- (2) IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance
- (3) IRM 10.8.6, Information Technology (IT) Security, Application Security and Development
- (4) NIST 800-53 Revision 5: Security and Privacy Controls
- (5) Modernizing Government Technology Act (MGT), December 2017
- (6) Government Accountability Office
- (7) Treasury Inspector General Tax Administration (TIGTA)
- (8) Presidential American Technology Council, 2017
- (9) Clinger-Cohen Act of 1996
- (10) Director of Office of Management and Budget (OMB)
- (11) Secretary of the Department of Homeland Security (DHS)
- (12) Federal Information Security Modernization Act (FISMA), 2014
- (13) Secretary of Commerce for modernization of Federal IT
- (14) 21st Century Integrated Digital Experience Act (IDEA), December 2018
- (15) SP 800-37 R2, Risk Management Framework for Information Systems and Organizations

2.5.1.1.3
(06-06-2022)
Roles and Responsibilities

- (1) **Information Technology (IT), Cybersecurity:** Cybersecurity manages the IRS IT Security program in accordance with the Federal Information Security Management Act with the goal of delivering effective and professional customer service to business units and support functions within the IRS. These services are the following:
 - a. Provides valid risk mitigated solutions to security inquisitions.
 - b. Ensure all IT security policies and procedures are actively developed, and updated.
 - c. Respond to incidents quickly, and effectively to eliminate risks/threats.
 - d. Provide security advice to IRS constituents, and monitor IRS robust security program for any required modifications or enhancements.

- (2) **Enterprise Operations (EOps):** EOps provides efficient, cost effective, secure and highly reliable computing server and mainframe services for all IRS business entities and taxpayers. EOps is responsible for the key services as follows:
- a. **Data Management Service and Support (DMSS):** Provides reliable database and storage operations by pioneering improvements in data services.
 - b. **Demand Management and Project Governance (DMPG):** Leads the management and support of mainframe technologies.
 - c. **Enterprise Computing Center (ECC):** Manages EOps technology support throughout the production life-cycle of the service and application infrastructure. ECC also executes IT management processes and procedures established by IT controls and oversight.
 - d. **Enterprise Server Division (ESD):** Leads the management and support of mainframe technologies.
 - e. **Enterprise Technology Implementation (ETI):** Focuses on maturing EOps support for new or high-profile services such as Portals, Share-Point, Cloud, Office 365, Windows 2019, Oracle, WinOS Migration, Tech Insertion, Aged Infrastructure, E-Discovery, eRecords and Program Management Framework. Includes Technology Implementation Services and IRS Web Infrastructure Services
 - f. **Infrastructure Services Division (ISD):** Drives operational technology solutions through broad-based knowledge of EOps infrastructure and systems.
 - g. **IT Operations Command Center (IT OCC):** Serves as EOps' first line of defense for Incident Management and Service restoration.
 - h. **Security Operations & Standards Division (SOSD):** Provides comprehensive oversight and management of EOps' IT Security program.
 - i. **Service Delivery Management (SDM):** Provides program management in support of high visibility, strategic IT initiatives that require coordination within and / or outside EOps.
 - j. **Server Support & Services Division (SSSD):**
 - Provisions servers for all platforms including the installation & configuration of COTS products
 - Provides product support for IBM Rational tools, monitors server capacity & conducts performance testing
 - Develops and manages standards for server Operating Systems and COTS products in the Tier 1 and Tier 2 environments
 - Supports verification and validation of newly provisioned servers
- (3) **Applications Development (AD):** AD is responsible for building, testing, delivering, and maintaining integrated information applications systems, e.g., software solutions, to support modernized systems and production environment to achieve the mission and objectives of the Service. Additionally, AD is responsible for the following:
- a. Works in partnership with customers to improve the quality and deliver changes to IRS information systems products and services.
 - b. A key component of tax processing/filing season activities.
 - c. Provides development support for administrative systems related to workforce support, human capital, financial, and facilities.

- d. Establishes and maintains rigorous contract and fiscal management, oversight, quality assurance, and program risk management processes to ensure that strategic plans and priorities are being met.
 - e. Maintains the effectiveness and enhance the integration of IRS installed base production systems and infrastructure while modernizing core business systems and infrastructure.
 - f. Provides quality assessment and assurance of Enterprise Life Cycle deliverables and processes.
- (4) Application Development's chain of command is the following:
- a. **Commissioner:** Oversees and provides overall strategic direction for the IRS. The Commissioner's and Deputy Commissioner's focus is for the IRS's services programs, enforcement, operations support, and organizations. Additionally, the Commissioner's vision is to enhance services for the nation's taxpayers, balancing appropriate enforcement of the nation's tax laws while respecting taxpayers' rights.
 - b. **Deputy Commissioner Operation Support (DCOS):** Oversees the operations of IRS-Wide Shared Services: Chief Financial Officer, Human Capital Office, Information Technology, Planning Programming and Audit Oversight and Privacy, and Governmental Liaison and Disclosure.
 - c. **Chief Information Officer (CIO):** The CIO leads Information Technology, and advises the Commissioner on Information Technology (IT) matters, manages all IRS Information Technology resources, and is responsible for delivering and maintaining modernized information systems throughout the IRS. Assisting the Chief Technology Officer (CTO) is the Deputy Chief Information Officer for Operations.
 - d. **Application Development (AD) Associate Chief Information Officer (ACIO):** The AD ACIO reports directly to the CIO; oversees and ensures the quality of: building, unit testing, delivering and maintaining integrated enterprise-wide applications systems to support modernized and legacy systems in the production environment to achieve the mission of the Service.
 - e. **Deputy AD Associate CIO (DACIO):** The Deputy AD ACIO reports directly to the AD ACIO, and is responsible for:
 - Leading all strategic priorities to enable the AD Vision, IT Technology Roadmap and the IRS future state.
 - Executive planning, and management of the development organization which ensures all filing season programs are developed, tested, and delivered on-time and within budget.
- (5) AD has the following Domains:
- a. Compliance Domain
 - b. Corporate Data Domain
 - c. Customer Service Domain
 - d. Data Delivery Service (DDS) Domain
 - e. Delivery Management Quality Assurance (DMQA) Domain
 - f. Identity & Access Management (IAM) Domain
 - g. Internal Management Domain
 - h. Submission Processing Domain
 - i. Technical Integration (TI) Domain

- (6) **Director, Compliance:** Provides executive direction for a wide suite of Compliance domain focused applications and oversee the IT Software Development organization to ensure the quality of production ready applications.
- a. Directs and oversees a unified cross-divisional approach to compliance strategies needing collaboration pertaining for the following:
- Abusive tax avoidance transactions needing a coordinated response
 - Cross-divisional technical issues
 - Emerging issues
 - Service-wide operational procedures
- (7) **Director, AD Corporate Data:** Directs and oversees the provisioning of authoritative databases, refund identification, notice generation, and reporting.
- (8) **Director, Customer Service:** Directs and oversees Customer Service Support for service and communication with internal and external customers and providing taxpayers with self-service online capabilities.
- a. Customer Service Domain's applications and systems provide:
- Tax law assistance
 - Taxpayer education
 - Access to taxpayer account data
 - Maintenance of modernized information systems that meet the customer's needs for researching, updating, analyzing, and managing taxpayer accounts
- b. Services to internal and external customers are provided through five primary means:
- Centralized Contact Centers (for telephone, written, and electronic inquiries)
 - Self-service applications (via the telephone and Internet)
 - Field Assistance (for walk-in assistance)
 - Web Services
 - Management of Taxpayer Accounts
- (9) **Director, Data Delivery Services:** Oversees and ensures the quality of data with repeatable processes in a scalable environment. The Enterprise Data Strategy is to transform DDS into a data centric organization dedicated to deliver Data as a Service (DaaS) through:
- **Innovation** - New methods and discoveries
 - **Renovation** - Streamline or automate
 - **Motivation** - Incentivize and enable individuals
- (10) **Director, Delivery Management & Quality Assurance (DMQA):**
- Executes the mission of DMQA by ensuring AD has a coordinated, cross-domain, and cross-organizational approach to delivering AD systems and software applications
 - Reports to the AD ACIO, and chairs the AD Risk Review Board
 - For additional information concerning AD roles, see Exhibit 2.5.1-2
- (11) **Director, Identity & Access Management (IAM) Organization:** Provides oversight and direction for continual secure online interaction by verification

and establishing an individual's identity before providing access to taxpayer information "identity proofing" while staying compliant within federal security requirements.

- (12) **Director, Internal Management:** Provides oversight for the builds, tests, deliveries, refund identification, notice generation, and reporting.
- (13) **Director, Submission Processing:** Provides oversight to an organization of over 17,000 employees, and is responsible for the processing of more than 202 million individual and business tax returns through both electronic and paper methods. Submission Processing is comprised of the following:
 - A headquarters staff responsible for developing program policies and procedures
 - Five Wage and Investment (W&I) processing centers
 - Seven commercially operated lockbox banks
- (14) **Director, Technical Integration:** Provides strategic technical organization oversight ensuring applicable guidance, collaboration, and consolidation of technical integration issues and quality assurance for the Applications Development portfolio.

2.5.1.1.4
(06-06-2022)

**Program Management
and Review**

- (1) The Enterprise Program Management Office (EPMO) is responsible for the delivery of integrated solutions for several of the IRS's large, scaled programs. It plays a key role in establishing change, release plans, and implementing new information system functional capabilities.
- (2) The EPMO is the primary partner with the business for programs under their purview and works with IT delivery partners (AD, ES, EOPs and the other ACIO areas) to deliver required capabilities. This structure positions each organization to maintain a strong core function to optimize their operations.

2.5.1.1.5
(06-06-2022)

Program Controls

- (1) The Enterprise Program Controls (EPC) Office leads the EPMO in Information Technology Enterprise-wide program management functions, and must assist other IT Applications Development (AD) organizations in cross domain support for a variety of program management disciplines.
- (2) The EPC office is comprised of six sections:
 - Enterprise Organizational Readiness (EOR)
 - Investment and Risk Management (I&RM)
 - Program Control and Integration (PC&I)
 - Program Management Office Support Services (PMOSS)
 - Program Operations (PO)
 - Program Support Services (PSS)
- (3) EPMO is essential to the strategic portfolio planning and enterprise portfolio management because it assists with the monitoring and management of IT spending and delivery.

#

- 2.5.1.1.6
(06-06-2022)
**Acronyms/Definitions/
Terms**
- (1) For terms and definitions see Exhibit 2.5.1-1
- (2) For acronyms see Exhibit 2.5.1-4
- 2.5.1.1.7
(06-06-2022)
Resources
- (1) This subsection describes the Internal Revenue Manual (IRM) that constitutes IRM Part 2 (Information Technology), Chapter 5 System Development). This section also identifies the Internal Revenue Service documents used with this IRM and any other documents associated with this IRM. The controls established in this IRM are based on concepts, principles, and theory expressed in the following references:
- a. IRM 2.5.3, Information Technology, System Development, Programming and Source Code Standards
 - b. IRM 2.5.4, Information Technology, System Development, Document Standards
 - c. IRM 2.5.6, Information Technology, System Development, Enhanced Software Development Life Cycle
 - d. IRM 2.5.8, Information Technology, System Development, Performance Measures
 - e. IRM 2.5.9, Information Technology, System Development, Peer Review
 - f. IRM 2.5.10, Information Technology, System Development, Function Point Standards
 - g. IRM 2.5.11, Information Technology, System Development, Analysis Techniques and Deliverables
 - h. IRM 2.5.12, Information Technology, System Development, Design Techniques and Deliverables
 - i. IRM 2.5.13, Information Technology, System Development, Database Design Techniques and Deliverables
 - j. IRM 2.5.14, Information Technology, System Development, Quality Assurance
 - k. IRM 10.5.8, Security Privacy and Assurance Privacy and Information Protection, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments
 - l. IRM 2.150.1, Information Technology, Configuration Management, Configuration Management Policy
 - m. IRM 2.150.2, Information Technology, Configuration and Change Management, Configuration Management
 - n. ISO/IEC 20000-1:2011, Information Technology - Service Management - Part 1: System Requirements, 9.2 Change Management
 - o. IT Infrastructure Library (ITIL) Service Transition, 2011 Ed., Chapter 4.2 Change Management
- (2) Other publications in this Internal Revenue Manual (IRM) are based on decisions, direction, guidance, or recommendations expressed in the following documents:
- a. Capability Maturity Model Integration (CMMI) Version 2.0 for Development, CMMI institute released March 2018, website: <https://cmmiinstitute.com>
 - b. GAO-21-524T - Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems report, April 2021
 - c. GAO-18-298T - Investment Performance and Risk Tax Processing report, June 2018

- d. Interim Guidance memo, "IT-02-1121-0010" IT Decommission Policy

2.5.1.2
(06-06-2022)

**System Development
Quality Assurance (QA)**

- (1) The Quality Assurance (QA) Program Office supports the delivery of high-quality products and services by ensuring projects remain within quality standards as established by the IRS. Currently there are eight process areas and three types of audits currently covered by the AD QA.
- (2) The QA process areas are as follows:
 - a. Project Planning
 - b. Project Monitoring and Control
 - c. Configuration Management
 - d. Requirements Management
 - e. Measurement and Analysis
 - f. Software Development
 - g. Testing
 - h. Supplier Agreement Management
- (3) QA audit types are as follows:
 - a. Process Audit - Evaluates a process area based on organizational standards and requirements.
 - b. Work Product Audit - Evaluates work products for conformance to the Enterprise Life Cycle (ELC), Data Item Descriptions (DID) and templates.
 - c. Release Review Audit - Evaluates a selection of processes used and work products created during a release.

2.5.1.2.1
(06-06-2022)

Configuration Controls

- (1) A Configuration control is an important function of the **Configuration Management** discipline. Its purpose is to ensure that all changes to a complex system are performed with the knowledge and consent of management. The scope creep that results from inefficient or nonexistent configuration control is a common cause of project failure.
- (2) Configuration control is an essential aspect of your project's Risk Management strategy. For example:

Example: Scope Creep Scenario: A project misses key milestones and does not produce any deliverables.

Reason: The software developer creates "9 new changes" to the software project to impress the customer without consulting the project manager or leadership.

Solution: Implement Configuration Control. Document all Request For Change (RFC), and have them reviewed and approved by a Configuration Control Board.

- (3) Configuration control has four main processes:
 - a. Identification and documentation of a change.
 - b. Analysis and evaluation of a Change Request.
 - c. Approval or disapproval of a Change Proposal.
 - d. Verification and validation, implementation and release of a change.

- (4) A critical aspect of the Change Control process is documenting changes, the more information contained in the documentation, the easier it is complete an assessment, development, maintenance, and improvement of the process controls.
- (5) The Configuration Control controls the changes to the design, structure, format, and manages the product (projects deliverables) throughout the lifecycle of the product.
- (6) Ensure all changes to the configuration items are controlled. Uncontrolled modifications to software requirements introduce the risk of cost and schedule overruns.

2.5.1.2.1.1
(06-06-2022)
Configuration Control Board

- (1) The Configuration Control Board (CCB) must:
 - a. Control the product and service baseline.
 - b. Evaluate and approve or reject proposed changes to the Configuration Item number.
 - c. Schedule the changes for upcoming releases.
- (2) Any new CCBs, subordinate CCBs, or exceptions must obtain approval from the Configuration Management process owner, see IRM 2.150.1 Configuration Management Policy.

2.5.1.2.1.2
(06-06-2022)
Government Sponsor, Configuration Control Board (CCB)

- (1) The Configuration Control Board controls the product and service baseline, and concurs on the distribution of all Work Requests resulting in approvals on the CCB SharePoint site.
- (2) The Government Sponsor approves, or disapproves Work Requests (WR), or deviations from controls cited under IRM 2.150.2 Configuration Management Process.

2.5.1.2.1.3
(06-06-2022)
Chairperson, Configuration Control Board (CCB)

- (1) The Configuration Control Board Chairperson approves or disapproves the proposed solution to a {change or governance decision} that exceeds a subordinate board's threshold and is within the (CCB, Governance or hybrid board) threshold.
- (2) The Configuration Control Board consist of the following:
 - a. AD CCBs
 - b. Domain CCBs
 - c. Branch CCBs
 - d. AD, Data Management Quality Assurance (QA)
 - e. Enterprise Architecture (EA)
 - f. Enterprise Operations, Investment Management and Change Control Board (IMCCB)

2.5.1.2.2
(06-06-2022)
Work Requests

- (1) Without approval from the Configuration Control Board (CCB), Work Requests or deviations from the process controls established under Internal Revenue Manual (IRM) Part 2 Information Technology, Chapter 5 Applications Development are not authorized.

- 2.5.1.3
(06-06-2022)
Configuration Management (CM)
- (1) Configuration Management (CM) is a critical control and discipline process for maintaining information about configuration items required to deliver an IT Service, and ensure the integrity, security, and reliability of information systems.
 - (2) CM's purpose is to identify, control, record, report, audit, and verify configuration items and to manage deviations from these controls, IRM 2.150.1 Information Technology, Configuration Management, Configuration Management Policy, establishes the following procedures:
 - Proposing a Change
 - Requesting a Work Request
- 2.5.1.3.1
(06-06-2022)
Change Management (ChM)
- (1) The purpose of Change Management (ChM) is to mitigate risk and impacts during the authorization process to approve any changes being deployed. This process controls the lifecycle of all changes while protecting the production environment during execution of any new changes.
- 2.5.1.3.1.1
(06-06-2022)
Organizational Change Management (OCM) Model
- (1) Organization Change (OCM) is a critical approach to managing the personnel side of change. OCM is critical for determining the origin of the resistance to change which shall keep all stakeholders and sponsors on board with major objectives.
 - (2) The **ADKAR** model is an acronym and useful tool that represent five milestones required for achieving successful change that contribute to coping and planning for the process. The ADKAR milestones are the following:
 - a. **A - Awareness:** Demonstrate the need for change: Explain **what** and **why** of the change.
 - b. **D - Desire:** Participate and support the change.
 - c. **K - Knowledge:** Personnel must know how to change by:
 - Obtaining training if necessary
 - Communicating the need and involving people in developing the change
 - Developing and accept the change plans
 - Implementing change plans
 - Performing an assessment of the progress
 - d. **A - Ability:** Consistently implement required skills for change.
 - e. **R - Reinforcement:** Consistently monitor the progress toward reinforce and sustain change. This prevents reverting back to previous ways.
- 2.5.1.3.2
(06-06-2022)
Proposing a Change
- (1) Personnel affected by controls cited under IRM, Part 2 Information Technology, Chapter 5 Applications Development, may propose a change to controls.
 - (2) The types of process changes are the following:
 - a. **Emergency Change:** A Request-For-Change (RFC) must be submitted for the change to occur as soon as possible as a (P1) or (P2) Incident Management ticket to the Change Analyst.

Example - Emergency Change

Example of Emergency Change	
Emergency Change	<p>An urgent change that could result in high risks if it is not addressed rapidly.</p> <ul style="list-style-type: none"> • Examples: security threats, power outages, system outages • Resolving a major incident • Implementing a security patch

- b. **Standard Change:** A Request-For-Change (RFC) must be submitted when an accepted solution from authority was approved in advance. This process pertains to repetitive or reoccurring changes.

Example - Standard Change

Example of Standard Change	
Standard Change	<p>A low-risk, commonly repeated, well-defined, and pre-approved process. This change has already gone through the risk assessment process</p> <p>Examples:</p> <ul style="list-style-type: none"> • Adding memory or storage • Creating a new instance of a database • Service desk request for an IT service

- c. **Normal Change:** A Request-For-Change (RFC) that requires a service change to a service or IT infrastructure. This is not an Emergency or Standard change, and is subject to a full change management review and Change Advisory Board review for authorization/rejection.

Example - Normal Change

Example of Normal Change	
Normal Change	<p>An intermediary-risk change that is not urgent or pre-approved. A thorough review process is conducted before approving.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Upgrading from an on-premises system to a cloud-based management system. • Migrating from an old system to a new system. • Performance improvements.

- (3) To propose a change, the steps are:

- a. **Proposer:** The proposer must prepare a proposal and submit the proposal to the Change Analyst.
- b. **Change Analyst (CA):** A Change Analyst is delegated by the Change Coordinator, and must manage/support the: plan, design, and build/test tasks of an RFC within the Change Management Life Cycle.
- c. The CA must also perform the following:
 - The impacted projects must be submitted as comments for the proposal to the responsible Change Analyst.
 - The Change Analyst must review the proposal to determine the impacted projects.
 - The Change Analyst must route the proposal with impacted projects for review.
 - The Change Analyst must package the proposal as a Work Request (WR) and submit the WR to the Coordinator.
 - The Change Analyst's Frontline Manager must review and authorize the RFC after it is submitted by the initiating Change Analyst.
- d. **Change Manager (ChM):** The Change Manager must support the Technical Authorization and Schedule and Approve Phases by reviewing the submitted Request For Change (RFC). The CM must ensure the RFC follows the correct workflow.
- e. **Change Coordinator (CC):** The Change Coordinator must coordinate the RFC/WR assessment, planning, and performance of work completed by the technical team.
- f. **Change Authority (CA):** The Change Authority is the approval group that must accept or reject the RFC/WR during the presentation to the Configuration Control Board (CCB). If the CA accepts the RFC/WR, the Chairperson must present the RFC/WR to the Committee or schedule the Proposer, Analyst, or Coordinator to present the RFC/WR.
- g. **Work Request (WR):** For WR the following must happen:
 - The Committee must reject or accept the WR
 - If the Committee accepts the WR, the Analyst must package the WR with signatures, then submit the package to CCB SharePoint site
- h. **Change Approver/Change Advisory Board (CAB):** The Change Approver or Change Advisory Board (CAB) consist of representatives from all IRS IT organizations/domains that must provide advice on the assessment, prioritization, scheduling of changes, and approval of releases.

- (4) For additional information pertaining to Change Management, see IRM 2.125.2 Information Technology, Change Management, Change Management Process Description.

2.5.1.3.3
(06-06-2022)
Requesting a Work Request

- (1) Personnel affected by controls cited under Internal Revenue Manual (IRM), Part 2 (Information Technology), Chapter 5 (Applications Development) may request a Work Request from these controls. If conformance to a control is impossible, unreasonable, or otherwise not in the best interest of the IRS, then a Work Request from conformance may be requested.
- (2) To request a Work Request, the steps are:
 - a. The Requestor must prepare a memo requesting the Work Request.
 - b. The Requestor must submit the memo to the Configuration Controls.

- c. The Coordinator must review the Work Request and submit the Work Request to the Sponsor, Configuration Control Board (CCB), for approval or denial.
 - d. The Government sponsor, CCB must either approve or deny the Work Request.
 - e. The Coordinator, within 15 working days, must notify the Requestor of a decision.
- (3) When preparing a memo to request a Work Request, at a minimum, the memo must:
- a. Identify the related standards document and, if applicable, the specific standard.
 - b. Explain and justify the request for a Work Request.
 - c. Identify any pertinent documentation.
 - d. Describe an alternative to the waived standard.
 - e. Identify a contact.
- (4) When notifying the Originator of a decision, at a minimum, the notification must:
- a. State whether the request was approved or denied or state whether additional time is required for a decision.
 - b. If additional time is required, then the notification must state the expected date of decision.
 - c. State an explanation to the Originator when a request is denied.

2.5.1.4
(06-06-2022)
Directives

- (1) This section establishes directives for System Development. Through internal controls and during the engineering, development, and maintenance of IRS software systems, these directives must be satisfied. Exhibit 2.5.1-4, for each directive, lists the IRMs that support the directive.
- (2) This IRM establishes the following directives:
- a. Assurance of Quality Software
 - b. Coordinate Change and Maintenance of Applications Configuration Controls
 - c. Coordinate Change of Applications
 - d. Curtail Software Defects
 - e. Define Applications Configuration Controls
 - f. Engineer Software Products
 - g. Integrate Engineering and Managerial Activities
 - h. Manage Requirements
 - i. Manage Software Changes
 - j. Manage Software Contracts
 - k. Plan Applications Change Projects
 - l. Track and Oversee Applications Change Projects
 - m. Plan/Define Continuous Process Improvement
 - n. Manage security controls for system development based on NIST 800-37 Risk Management Framework and NIST 800-53 Revision 5: Security and Privacy Controls
 - o. Plan/Define Organizational Process Training

2.5.1.4.1
(06-06-2022)

**System Development
Quality Assurance (QA)
Best Practices**

- (1) The purpose of this directive is to provide management with visibility into the processes being used by organizational units that develop, maintain, and manage software.
- (2) The following requirements state what is expected to satisfy this directive:
 - a. All activities for Quality Assurance (QA) must be planned.
 - b. Quality Assurance must be applied to all Application Change projects.
 - c. Software product quality (the conformance of products with standards and requirements) must be objectively validated.
 - d. Software service performance (the adherence of services with procedures and requirements) must be objectively verified.
 - e. Organizational units affected by QA activities must be informed of these activities and the results.
 - f. Noncompliance issues unresolved among organizational units must be organizationally elevated and resolved.

2.5.1.4.1.1
(06-06-2022)

Audit Process Control

- (1) The Quality Assurance Program conducts audits for organizational process areas as outlined in IRM 2.5.14 System Development, Quality Assurance. AD Quality Assurance is responsible for thirteen process areas, and three types of audits for process control:
 - a. The thirteen process areas are:
 - Project Planning (PP)
 - Project Monitoring and Control (PCM)
 - Configuration Management (CM)
 - Quality Assurance (QA)
 - Requirements Engineering (RQEN)
 - Risk Management (RSKM)
 - Process Management (PRM)
 - Privacy (PRIV)
 - Section 508 (508)
 - Security (SEC)
 - Software Development (SWDEV)
 - Supplier Agreement Management (SM)
 - Testing (TEST)
 - b. The three audit process controls are:
 - Process Area Audit
 - Work Product Audit
 - Process Owner Audit
- (2) The final Audit Findings report is issued and stored in the QA repository, and when audit findings need corrective action, a Corrective Action plan is requested from the auditor as a part of the Audit Findings report.

2.5.1.4.2
(06-06-2022)

**Coordinate Change and
Maintenance of System
Change Control**

- (1) The IT Enterprise Operations, Demand Management & Project Governance (DMPG) Change Advisory Board (CAB) is a community of IT executives and IT professionals that advise and collaborate with the Application Development domain for the assessment, prioritization, scheduling of changes, and the approval of releases.

- (2) The purpose of this directive is to establish organizational responsibility for activities that improve the IRS's capability to develop systems and software applications. The following requirements state what is expected to satisfy this directive:
 - a. System Change and improvement activities must be coordinated across the organization.
 - b. Strengths and weaknesses of the Change processes used must be identified relative to the standard processes.
 - c. Organization-level Change processes, and improvement activities must be planned.
- (3) For more information on the overall Change Management process see, IRM 2.125.1 Change Management, Change Management Policy and IRM 2.125.2 Change Management Process Description.

2.5.1.4.3
(06-06-2022)
Coordinate Change of Software

- (1) The purpose of this directive is to establish a means for the system development Change Management processes to participate with the other Change groups so that the project is better able to satisfy the customer's needs. The Demand Management & Project Governance (DMPG) is responsible for the development, implementation, and maintenance of this process. The following requirements state what is expected to satisfy this directive:
 - a. The customer's business requirements must be agreed to and signed by all affected organizations.
 - b. Commitments among the Change organizations must be agreed to by affected organizations.
 - c. Development organizations must identify, track, and resolve issues.

2.5.1.4.4
(06-06-2022)
Curtail Software Defects

- (1) The purpose of this directive is to remove defects from software early and efficiently. The following requirements state what is expected to satisfy this directive:
 - a. Planning and coordination of requirements.
 - b. Peer review meetings must be planned.
 - c. Defects in software products must be identified by total number of major and minor defects found by all peer reviewers and removed.
 - d. Rework must be performed to resolve issues found.
 - e. A follow-up peer review meeting must be performed for reworked requirements artifact.
 - f. Exit Criteria - All defects and issues have been identified, corrected, and the product is accepted.

2.5.1.4.5
(06-06-2022)
Define System Configuration Controls

- (1) The purpose of this directive is to develop and maintain a usable set of system Change Process assets and controls that improve process performance across the organization and that provide a basis for cumulative, long-term benefits to the organization. The following requirements state what is expected to satisfy this directive:
 - a. A standard Change and Maintenance process for the organization must be developed and maintained.
 - b. Information about the organization's use of standard processes must be collected, organized, reviewed, and shared.

- 2.5.1.4.6
(06-06-2022)
Engineer Software Products
- (1) The purpose of this directive is to consistently perform a well-defined engineering process that integrates all software engineering activities, effectively and efficiently, to produce correct, consistent software products. The following paragraphs state what is required to satisfy this directive:
- a. Software engineering tasks/activities must be defined, integrated, and consistently performed to produce software.
 - b. Software products must be kept consistent.
- 2.5.1.4.7
(06-06-2022)
Integrate Engineering and Managerial Activities
- (1) The purpose of this directive is to integrate the software engineering and management activities into a coherent, defined process that is tailored from the organization's Configuration Controls. The following requirements state what is expected to satisfy this directive:
- a. Project plans must be tailored from the IRS's standard Change processes.
 - b. Projects must be planned and managed according to the IRS's standard Change processes.
- 2.5.1.4.8
(06-06-2022)
Improve Processes and Maintain Process Assets
- (1) The purpose of this directive is to receive, evaluate, review, and implement new improved, or enhanced processes then implement best practices. The following requirements state what is expected to satisfy this directive for Continuous Process Improvement (CPI):
- a. Establish the framework for organizations to make incremental process improvements.
 - b. Establish and maintain a set of organizational process assets.
 - c. Plan, implement, and communicate improvements.
 - d. Coordinate and deploy Process Change and improvement activities across the organization.
 - e. Develop new and updated processes and process assets.
- 2.5.1.4.9
(06-06-2022)
Manage Requirements
- (1) The purpose of this directive is to establish a common understanding of the requirements allocated to the software between an organizational unit that is acquiring software and an organizational unit that is developing or maintaining the software. The following requirements state what is expected to satisfy this directive:
- a. System requirements allocated to software must be controlled to establish a baseline for software engineering and management.
 - b. When allocated requirements are changed, the plans, products, and activities associated with the software must be accordingly changed.
- 2.5.1.4.10
(06-06-2022)
Manage Software Configurations
- (1) The purpose of this directive is to establish and maintain the integrity of the product, throughout the life of the corporate software product. The following requirements state what is expected to satisfy this directive:
- a. Software configurations management activities must be planned.
 - b. Corporate software products, identified as software configuration items, must be cataloged, controlled, and inventoried.
 - c. Access to, changes to, and distribution of configuration items must be controlled.

- d. Organizational units involved in software configuration management activities must be informed of the status and content of software baselines.
- 2.5.1.4.11
(06-06-2022)
Manage Software Contracts
- (1) The purpose of this directive is to select qualified software contractors and effectively manage them. The following requirements state what is expected to satisfy this directive:
 - a. Documented standards and procedures must be used in selecting software subcontractors and managing the subcontract.
 - b. Project managers and subcontractors must agree to their commitments to each other.
 - c. Project managers and subcontractors must maintain ongoing communication.
 - d. Project managers must track contractor’s actual results and performance against commitments.

#

- 2.5.1.4.12
(06-06-2022)
Plan Applications Development Projects
- (1) The purpose of this directive is to establish reasonable plans for managing Change projects and performing engineering tasks. The following requirements state what is expected to satisfy this directive:
 - a. Estimates must be documented and used in project planning and tracking.
 - b. Project activities and commitments must be planned and documented.
 - c. Project commitments must be negotiated between all managers involved in a project and the results of this negotiation must be documented.

- 2.5.1.4.13
(06-06-2022)
Track and Oversee System Development and Software Development Projects
- (1) The purpose of this directive is to provide adequate visibility into the actual development progress so that management can take effective actions when the project’s performance deviates significantly from the plan (project plan or applications Change plan). The following requirements state what is expected to satisfy this directive:
 - a. Actual results and performance must be tracked against the project plan.
 - b. When actual results and performance significantly deviate from the plan, corrective actions must be taken and managed to closure.
 - c. Changes to project commitments must be agreed to by managers in affected organizational units.

- 2.5.1.4.14
(06-06-2022)
Define/Plan Organizational Process Training
- (1) The purpose of this directive is to develop the skills and knowledge of employees to perform their role effectively and efficiently. The following requirements state what is expected to satisfy this directive:
 - a. Training activities are planned.
 - b. Identify training needed by the organization.
 - c. Obtain and provide training to address those needs.
 - d. Establish and maintain training records.
 - e. Assess training effectiveness.

#

#

Exhibit 2.5.1-1 (06-06-2022)
Terms and Definitions

Terms	Descriptions
IRS Software System	A software system developed by or for the IRS.
Application	<ul style="list-style-type: none"> a. A collection of software programs that automates a business function, and its data provided by a taxpayer or third party to the IRS regarding the applicant’s status. b. Applications include IRS-specific functionality in support of business requirements as well as generic end-user functionality.
Audit	An independent examination of deliverables, products, or services performed to assess compliance with established policies, procedures, standards, processes or other controls.
Batch Applications	Manage data, and generate reports, etc., as part of a business process.
Capability Maturity Model	A description of the stages through which an organization or organizational unit evolves as it defines, implements, measures, controls, and improves its Change processes. By facilitating the determination of current capabilities and the identification of issues most critical to product quality and service performance, this model provides a guide for selecting improvement strategies.
CCB SharePoint	A SharePoint site that displays a change in Configuration Controls. The bulletin describes the change, justifies the change, states the benefits of implementing the change, identifies the affected Internal Revenue Manual, lists the organizational units/personnel that are affected and targeted for IRM document clearance, and identifies a contact for responses to the change.
Change Management Program	The objective of the ChM program is to create and deploy a standard ITIL Change Management process for all of IT, supported by an integrated change management system.
Continuous Improvement	Sometimes called continual improvement. The ongoing improvement of products, services, or processes through incremental and breakthrough improvements.
Continuous Process Improvement	Provides a framework for organizations to make incremental process improvements, even in those processes that are considered to be in good operating condition. It is based on the philosophy that organizations can always make improvements.
Control	<p>A statement published to either</p> <ul style="list-style-type: none"> 1) Determine or influence decisions 2) Establish limits, alternatives, and guidelines for personnel who exercise discretion in applying their authority or fulfilling their duties and responsibilities.
Customer	A person or organizational unit that is responsible for accepting a product or service and for authorizing payment to the provider.

Exhibit 2.5.1-1 (Cont. 1) (06-06-2022)
Terms and Definitions

Terms	Descriptions
Configuration Controls	Controls used to influence or determine decisions regarding the engineering, development, or maintenance of systems. In a managerial context, a Configuration Controls may constitute a policy, directive, standard, or procedure. In a technical context, a Configuration Controls may address a deliverable, method, process, technique, task, or tool.
Directive	A control that expresses executive commitment, direction, or leadership.
Enterprise Organization Readiness	Enterprise Organizational Readiness (EOR) ensures the preparedness of organizations through a proven framework to identify and drive the resolution of gaps in the focus areas of People, Process, Technology and Financial readiness with a joint partnership between IT Delivery Partners and Business stakeholders.
Enterprise Data Standards and Guidelines	IRS standards and guidelines for the development and modification of the names, definitions, and other metadata for classes, attributes, and data models.
End User	When a product or service is deployed in its operational environment, an end user refers to the person or organizational unit that will use the product or service for its intended operational use.
Findings	The conclusions of an assessment, evaluation, audit, or review that identify issues, problems, or opportunities within the area of investigation.
Focus group	A group, usually of 8 to 10 persons, that is invited to discuss an existing or planned product, service or process.
Generic Application Functionality	This includes common desktop applications, its functionality include highly complex capabilities that are nevertheless common to many different types of enterprise such as accounting or customer-relationship-management capabilities.
Generic Application Capability	Provided by COTS applications, whereas IRS-specific capabilities generally involve custom-developed applications.
Guideline	A control that is not monitored for compliance, or compliance is not mandatory.
Information Technology Infrastructure Library	A set of detailed practices for Information Technology (IT) Service management (ITSM) that focuses on aligning IT services with business objectives.
Method	A set of criteria and rules that establishes a consistent, predictable, or repeatable way to perform a task or produce a result.
Methodology	A synthesis of controls, methods, plans, or principles that constitutes an approach for accomplishing something.

Exhibit 2.5.1-1 (Cont. 2) (06-06-2022)
Terms and Definitions

Terms	Descriptions
Modernizing Government Technology Act	In 2017, the Modernizing Government Technology Act was enacted as part of the 2018 National Defense Authorization Act. It established the Technology Modernization Fund (TMF) and Board and authorized agencies to develop IT working capital funds to modernize and update systems over many years. However, that’s not exactly how things worked out.
Organization	An organizational unit that comprises other organizational units.
Organizational Unit	A group of people acknowledged as a unit within an organization.
Peer Review	A review of a deliverable/product performed by peers of the producers of the deliverable/product and performed to identify defects and improvements.
Procedure	A control used and enforced to establish uniform performance of some activity or service.
Process Improvement	An application of the plan-do-study-act (PDSA) philosophy to processes to produce positive improvement and better meet the needs and expectations of customers.
Process Improvement	A structured environment often made up of cross functional members who work together to improve a process or processes.
Program	<ul style="list-style-type: none"> • A group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually. • Programs may include elements of related work outside the scope of the discrete projects in the program. • A collection of related projects and the infrastructure that supports them, including objectives, methods, activities, plans, and success measures.
Program Management Office Support Services	Program Management Office Support Services (PMOSS) supports new and existing IT programs by providing program management best practices through leadership, individualized guidance, and easily accessible tools.
Program Operations	Program Operations (PO) is responsible for financial management and acquisition support to the Enterprise Program Management Office (EPMO) and the individual programs and projects that the EPMO provides sponsorship.
Program Support Services	Program Support Services (PSS) provides employee engagement development and support, SharePoint solutions and workforce planning efforts for the EPMO.

Exhibit 2.5.1-1 (Cont. 3) (06-06-2022)
Terms and Definitions

Terms	Descriptions
Project	A managed set of interrelated resources which delivers one or more products to a customer or end user. A group of tasks to accomplish a specific objective, with a beginning and ending date; and typically operates according to a plan. This plan is frequently documented, specifies the deliverables, resources, required funds, tasks, and schedule of work.
Project Manager	A role assigned to a person who is expected to manage a project and manage according to a budget, schedule, defined scope, and documented plan.
Software Application	A software product applied in some discipline or field (e.g., accounting, purchasing, project management) to accomplish work.
Software Product	The complete set or any of the individual items of the set, of computer programs, procedures, and associated documentation and data designated for delivery to a customer or end user.
Software System	A collection of software components organized to accomplish a function
Standard	A control that specifies a mandatory characteristic for some product or other result, and is enforced to prescribe a uniform quality for a product or other result
Sub-application	<p>a. A part of a larger application (please see definition for application above):</p> <ul style="list-style-type: none"> • Functionality supports business processes • Collection of one or more software programs that automates a business function • This can reference other sub-applications to any depth
Sub-project	A component of a larger project.
System	A collection of components organized to accomplish a specific function or set of functions.
System Requirement	A condition or capability that a system or system component must meet
Tailor	To modify a process, standard, or procedure.
Technology Modernization Board	The role of the Technology Modernization Board is to evaluate project proposals submitted for funding in accordance with the Modernizing Government Technology (MGT) Act.
Technology Modernization Fund	An innovative funding vehicle that gives agencies additional ways to deliver services to the American public more quickly, better secure sensitive systems and data, and use taxpayer dollars more efficiently.
Work Product	All products and deliverables including the standards/procedures used to produce them.

Exhibit 2.5.1-2 (06-06-2022)
Roles By Organizational Unit

This exhibit identifies the organizational units assigned to the roles established through this IRM. Where a role is assigned to an organizational unit, the assignment means the role is assigned to the manager of the unit, or person delegated by the manager.

Role	Organizational Unit
Change Control Board	Director, Delivery Management and Quality Assurance
	OS:IT:AD:DMQA
Configuration Control Board	Director, Corporate Data
	OS:CIO:AD:CP
	Director, Compliance Systems
	OS:CIO:AD:C
	Director, Internal Management Systems
	OS:CIO:AD:IM
	Director, Submission Processing
	OS:CIO:AD:SP
	Director, Customer Service
	OS:CIO:AD:CS
Sponsor, Configuration Control Board	Director, Technical Integration Organization
	OS:CIO:TIO
Chairperson, Configuration Control Board	Application Development
	OS:CIO:AD

Exhibit 2.5.1-3 (06-06-2022)**Directives and Supporting Internal Revenue Manuals**

Directive	IRM that supports Directive
Establishes standards and guidelines for development of maintainable, portable, reliable software applications	IRM 2.5.3, System Development, Programming and Source Code Standards
Guidelines on preparation of Enterprise Life Cycle documents that are the deliverable	IRM 2.5.4 , Document Standards
Establishes standards for conducting the QA audit process within Application Development (AD)	IRM 2.5.14, Quality Assurance
Establishes all components and infrastructure of the IRS EA	IRM 2.15.1, Enterprise Architecture (EA), EA Overview
Provides a standard for IRS ELC framework for managing, governing and supporting system tactics, architecture, IT security, and engineering.	IRM 2.16.1, Enterprise Life Cycle
OneSDLC transforms IT practices and optimize delivery of IT systems and applications at the IRS using Agile and Lean practices. IT product delivery is modernized through a single software development life cycle approach and delivery model. OneSDLC optimizes product, software and service delivery and reduces lead and cycle time through agile and lean processes and practices and is governed by tool-based content. The focus is on enterprise level transformation and driving efforts that will enable that transformation.	IRM 2.31.1 , One Software Development Life Cycle (SDLC)
Requirements Development and Requirements Management process areas	IRM 2.110.1, Information Technology, Requirements Engineering, Requirements Engineering Directive
Standard for planning and performing development and integration of IT based systems within the IRS.	IRM 2.120.1, Information Technology, Engineering, Engineering Policy
Standard Best practice for creating a set of procedures to obtain key processes for business objectives	IRM 2.110.2, Information Technology, Requirements Engineering, Requirements Engineering Process
Establishes standards for verification and validation activities for all phases of the testing life cycle.	IRM 2.127.1, Information Technology, Testing Standards and Procedures Testing Policy and IRM 2.127.2, Testing Standards and Procedures
Define System Development Configuration Controls	IRM 2.150.1, Information Technology, Configuration Management Policy

Exhibit 2.5.1-3 (Cont. 1) (06-06-2022)
Directives and Supporting Internal Revenue Manuals

Directive	IRM that supports Directive
Describes the formal Information Technology (IT) policy for implementing the requirements of the Change Management (ChM) process	IRM 2.125.1 Change Management, Change Management Policy
Establishes standards for the Change Management Process	IRM 2.125.2, Information Technology, Change Management Process Description
Establishes standards for creating data names and eliminating data redundancies	IRM 2.120.12, Information Technology, Data Engineering, Naming Data Element(s)/Object(s)

Exhibit 2.5.1-4 (06-06-2022)
Acronyms and Definitions

Acronym	Definition
ACIO	Assistant Chief Information Officer
AD	Application Development
ADKAR	Aware, Desire, Knowledge, Ability, Reinforcement
CCB	Change Control Board
CCB	Configuration Control Board
CIO	Chief Information Officer
ChM	Change Management
CMM	Capability Maturity Model
CR	Change Request
CMMI	Capability Maturity Model Integration.
CPI	Continuous Process Improvement
DCOS	Deputy Commissioner for Operations Support
EDSG	Enterprise Data Standards and Guidelines
ELC	Enterprise Life Cycle
EPC	Enterprise Program Controls
EPMO	Enterprise Program Management Office
EOR	Enterprise Organizational Readiness
IG	Interim Guidance
IRM	Internal Revenue Manual
I&RM	Investment and Risk Management
IRSD	Internal Revenue Service Document.
ITIL	Information Technology Infrastructure Library
PC&I	Program Control and Integration
PDCA	Plan-Do-Check-Act
PMOSS	Program Management Office Support Services
MGT Act	Modernizing Government Technology Act
OneSDLC	One Software Development Life Cycle
PSS	Program Support Services
QA	Quality Assurance
QC	Quality Control

Exhibit 2.5.1-4 (Cont. 1) (06-06-2022)
Acronyms and Definitions

Acronym	Definition
W&I	Wage and Investment
WR	Work Request.

