



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.07-02 v2024-02

Published: 2024-02-23

**Configuration Management
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	4
Document History Log	4
Approval	4
1. Introduction	5
1.1. Purpose	5
1.2. Scope	5
1.3. Point of Contact(s)	6
1.4. Applicability	6
1.5. Applicable Documents	6
1.5.1. Federal Information Processing Standards (FIPS)	6
1.5.2. National Institute of Standards and Technology (NIST)	6
1.5.3. National Aeronautics and Space Administration (NASA)	7
1.5.4. Cancellations or Updates	7
2. Security Controls, Corresponding Roles and Responsibilities	7
2.1. Configuration Management Policy and Procedures (CM-1)	7
2.1.1. Senior Agency Information Security Officer (SAISO)	7
2.1.2. Center Chief Information Security Officer (Center CISO)	7
2.1.3. Information System Owner (ISO)	7
2.2. Baseline Configuration (CM-2)	8
2.2.1. Center Chief Information Security Officer (Center CISO)	8
2.2.2. Information System Owner (ISO)	8
2.2.3. Information System Security Officer (ISSO)	8
2.3. Baseline Configuration I Retention of Previous Configurations (CM-2(3))	8
2.3.1. Information System Owner (ISO)	9
2.4. Baseline Configuration I Configure Systems and Components for High-Risk Areas (CM-2(7))	9
2.4.1. Center Chief Information Security Officer (Center CISO)	9
2.5. Configuration Change Control (CM-3)	9
2.5.1. NASA Security Operations Center (SOC)	9
2.5.2. Information System Owner (ISO)	9
2.6. Configuration Change Control I Test/ Validate/ Document Changes (CM-3(2))	10
2.6.1. Information System Security Officer (ISSO)	10
2.6.2. Information System Owner (ISO)	10
2.7. Impact Analysis (CM-4)	10
2.7.1. Information System Owner (ISO)	10
2.8. Access Restrictions for Change (CM-5)	10
2.8.1. Information System Owner (ISO)	10
2.9. Configuration Settings (CM-6)	11
2.9.1. Cybersecurity Standards and Engineering Team	11
2.10. Configuration Settings Automated Management, Application, and Verification (CM-6(1))	11
2.10.1. Office of the Chief Information Officer (OCIO)	11
2.10.2. Information System Owner (ISO)	11
2.11. Least Functionality (CM-7)	11
2.11.1. Information System Owner (ISO)	11
2.12. Least Functionality I Periodic Review (CM-7(1))	12
2.12.1. Information System Owner (ISO) and/or Information System Security Officer (ISSO)	12

2.13. Least Functionality I Prevent Program Execution (CM-7(2))	12
2.13.1. Information System Owner (ISO)	12
2.14. Least Functionality I Unauthorized Software/ Allow by Exception (CM-7(5))	12
2.14.1. Information System Owner (ISO) and/or Information System Security Officer (ISSO)	12
2.15. Information System Component Inventory (CM-8)	12
2.15.1. Office of the Chief Information Officer (OCIO)	12
2.15.2. Information System Owner (ISO)	13
2.16. Information System Component inventory I Updates During Installations/Removals (CM-8(1))	13
2.16.1. Office of the Chief Information Officer (OCIO)	13
2.16.2. Information System Owner (ISO)	13
2.17. Information System Component Inventory Automated Maintenance (CM-8(2))	13
2.17.1. Office of the Chief Information Officer (OCIO)	13
2.17.2. Information System Owner (ISO)	13
2.18. Information System Component Inventory I Automated Unauthorized Component Detection (CM-8(3))	14
2.18.1. Office of the Chief Information Officer (OCIO)	14
2.18.2. Information System Owner (ISO)	14
2.18.3. Information System Owner (ISO) and/or Center Chief Information Security Officer (Center CISO)	14
2.19. Configuration Management Plan (CM-9)	14
2.19.1. Information System Owner (ISO)	14
2.20. Software Usage Restrictions (CM-10)	15
2.20.1. Enterprise License Management Team	15
2.20.2. Information System Owner (ISO)	15
2.21. User-Installed Software (CM-11)	15
2.21.1. Senior Agency Information Security Officer (SAISO)	15
2.21.2. Information System Owner (ISO)	15
2.21.3. Information System Security Officer (ISSO)	15
2.21.4. NASA User	15
Appendix A: Acronyms	15

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Draft
1.1	2013-04-30	Extended for 1 year.
1.2	2014-04-24	Extended while revision 4 updates are rolled into the Handbook.
1.3	2014-12-01	Revised for Rev 4 controls and ODVs, updated TOC
1.4	2015-02-23	Revised ITSEC EW and wording in 6.1.4.1
1.5	2016-08-17	Updated CM-5 to align with GAO audit request
1.6	2017-02-14	Extended Handbook for updates
1.7	2017-03-14	Updated Handbook to: • Align with current NASA Handbook template • Align to NIST SP 800-53 revision 4 • Reflect new CM tools deployed in the NASA IT environment
1.8	2018-08-15	Updated to new Handbook format
1.9	2021-05-21	Annual review; updated responsible party from ETAD to CSET; updated ISO and added OCIO role to CM-06 and CM-08; minor grammatical edits.
1.10	2021-09-30	Update to reflect SP 800-53 Rev.5
1.11	2023-01-31	Annual validation and updates
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval

Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization ([FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*](#)), and in the selection and implementation of information security controls ([FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#) and [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)), in a manner consistent with the Risk Management Framework ([NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)).

[NPD 2810.1, *NASA Information Security Policy*](#), [NPR 2810.1, *Security of Information and Information Systems*](#), and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of [SP 800-53](#).

[NPR 2810.1](#) designates this Handbook as a guide of NASA's Configuration Management (CM) information security controls, and the content of this document, in conjunction with [NPD 2810.1](#) and [NPR 2810.1](#), defines NASA policy and procedures to address [CM-1](#).

This Handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.

The terms "shall" and "may" within this Handbook are used as defined in ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks.

1.1. Purpose

Configuration Management describes information system baseline configurations, establishing configuration reviews and validation, and change control. The control family also manages administrator roles, and the ability of individuals to make changes to the information systems' configuration. The concept of configuration management is critical to the continuous monitoring processes. Strict methodologies for the regulation of information system baselines and changes to system configurations are necessary to enable near real-time understanding of a system's risk posture.

1.2. Scope

The scope of this Handbook encompasses all NASA systems documented in the Risk Information Security Compliance System (RISCS).

The Agency Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) have authorized the Cybersecurity Standards and Engineering Team (CSET) via the Agency Security Configuration Standards (ASCS) initiative to create binding Specifications and Technical Standards related to Agency cybersecurity topics.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes CSET as a standards-developing organization within the Agency.

IT Handbooks, IT Security Handbooks, and NASA IT Requirements are issued by the Office of the Chief Information Officer (OCIO) and provide specific requirements to protect the confidentiality, integrity, and availability of NASA information and information systems. Pursuant to [NPR 1400.1, *NASA Directives and Charters Procedural Requirements*](#), Appendix D, these documents work in conjunction with NASA Policy Directives (NPDs) and NPRs by providing specific requirements to comply with relevant NPDs and NPRs governing NASA information and information systems. Handbooks are effective until formally cancelled, rescinded, or superseded by an updated document.

All NASA information and NASA information systems shall be managed in compliance with the requirements of CSET Specifications, CSET Technical Standards, IT Handbooks, IT Security Handbooks, and NASA IT Requirements in order to be authorized for use. Where necessary, information or information system owners, and program or project managers shall incorporate the requirements of CSET Specifications, CSET Technical Standards, IT Handbooks, IT Security Handbooks, and NASA IT Requirements into contracts and program or other agency documents to ensure that these requirements are followed.

All of these documents including handbooks, specifications and standards are available at: <https://cset.nasa.gov/ascs/>

This Handbook and the procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded, or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Chief Information Security Officers (Center CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hg-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the Center CISO, and directed to the attention of the point of contact for this Handbook to address and resolve.

1.4. Applicability

This Handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5. Applicable Documents

1.5.1. Federal Information Processing Standards (FIPS)

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

1.5.2. National Institute of Standards and Technology (NIST)

- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-128, *A Framework for Designing Cryptographic Key Management Systems*

1.5.3. National Aeronautics and Space Administration (NASA)

- [NPD 2810.1, NASA Information Security Policy](#)
- [NPR 2810.1, Security of Information and Information Systems](#)
- [NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories](#)
- [ITS-HBK-2810.11-02, Media Protection and Sanitization](#)
- [NASA-STD-2601, Minimum Cybersecurity Requirements for Computing Systems](#)
- [NASA-STD-2602, Security Requirements for Data at Rest \(DAR\)](#)
- [NASA-STD-2804, Minimum Interoperability Software Suite](#)
- [NASA-STD-2805, Minimum Hardware Configurations](#)
- [NASA-STD-2540.6, NASA Corporate Device Naming Convention](#)

1.5.4. Cancellations or Updates

- [ITS-HBK-2810.07-01, Configuration Management](#)

2. SECURITY CONTROLS, CORRESPONDING ROLES AND RESPONSIBILITIES

2.1. Configuration Management Policy and Procedures ([CM-1](#))

2.1.1. Senior Agency Information Security Officer (SAISO)

The SAISO:

- Develops, documents, and makes available to all persons:
 - A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
 - A plan and procedures to implement the configuration management policy and associated configuration management controls.
- Review and update the current:
 - Configuration management policy annually or if there is a major change.
 - Configuration management procedures annually or if there is a major change.

2.1.2. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Ensures Center-wide implementation of NASA policies and procedures that relate to configuration management.
- Reports systemic or significant risks to the SAISO or Center CIO.

2.1.3. Information System Owner (ISO)

The ISO:

- Reports all risks associated with deviations to the control requirements to the Authorizing Official (AO).

2.2. Baseline Configuration (CM-2)

2.2.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Ensures that the Center utilizes and complies with Agency baseline configuration guidelines.
- Reports systemic or significant risks to the SAISO or Center CIO.
- Tracks and reports on Risk Based Decisions (RBD).

2.2.2. Information System Owner (ISO)

The ISO:

- Ensures their systems comply with all IT security baselines and prevents those systems from connecting to a NASA network if they do not comply with IT security baselines or other relevant Agency mandates.
- Maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.
- Develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
- Employs configuration management at a level appropriate with the size, complexity, and sensitivity of the system to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
- Reviews and updates the baseline configuration of the information system:
 - Annually.
 - When required due to major change or upgrade.
 - As an integral part of information system component installations and upgrades.
 - When an updated ASCS Security Specification pertaining to the system or software is released.

2.2.3. Information System Security Officer (ISSO)

The ISSO:

- Ensures security baseline configurations conform to Cybersecurity Standards and Engineering Team (CSET) Agency Security Configuration Standards (ASCS) at Agency Security Configuration Standards (nasa.gov) and enforces compliance with those Standards.
- Ensures that a naming standard for all NASA devices is utilized for security purposes.
- Every device shall consist of a name that starts with the two-letter facility abbreviation followed by a unique string, which is approved and registered with the EDW project. The string shall correspond with the NASA security plan and consist of multiple strings. The same strings shall not be used by multiple security plans except during a transition phase.

2.3. Baseline Configuration I Retention of Previous Configurations (CM-2(3))

2.3.1. Information System Owner (ISO)

The ISO:

- Retains previous versions of baseline configurations to support rollback to the previous system state in the event of a system issue or failure.

2.4. Baseline Configuration I Configure Systems and Components for High-Risk Areas (CM-2(7))

2.4.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Issues loaner laptop with basic configuration to individuals traveling outside of the United States or to locations that the organization deems to be of significant risk in accordance with NASA policy guidance on Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories; and applies appropriate wiping methodology to the devices when the individuals return, in accordance with [ITS-HBK-2810.11-02, Media Protection and Sanitization](#).

2.5. Configuration Change Control (CM-3)

2.5.1. NASA Security Operations Center (SOC)

The NASA Security Operations Center (SOC):

- Ensures unauthorized security-relevant configuration changes are documented as IT security incidents in the NASA Incident Management System (IMS).

2.5.2. Information System Owner (ISO)

The ISO:

- Ensures that information systems are equipped with Agency-defined configuration status monitoring, and patch management and reporting tools.
- Reviews proposed configuration-controlled changes to the information system.
- Documents any and all deviations from baseline configurations, as defined by ASCS standards.
- Determines and documents the types of changes to the information system that are configuration controlled.
- Implements approved configuration-controlled changes to the information system.^[1]
- Retains records of configuration-controlled changes to the information system for one year.
- Audits and reviews activities associated with configuration-controlled changes to the information system.
- Coordinates and provides oversight for configuration change control activities for all changes.
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
- Ensures the capability to audit information systems in order to detect unauthorized changes in a manner consistent with organization-defined values (ODVs).
- Obtains approval from the Center CISO and/or appropriate AO for systems that cannot be equipped with Agency-defined configuration status monitoring, and patch management and reporting tools.

- Determines, in collaboration with the Center CISO or ISSO, if detected changes in configuration settings are the result of an incident to be reported to the NASA SOC

2.6. Configuration Change Control I Test/ Validate/ Document Changes (CM-3(2))

Individuals/groups conducting tests must follow NASA security policies and procedures, including those specific to information system security, and understand the specific health, safety, and environmental risks associated with particular facilities and processes.

2.6.1. Information System Security Officer (ISSO)

The ISSO:

- Confirms that all configuration changes are documented in the system's security documentation (e.g., System Security Plan) in a manner consistent with ODVs.

2.6.2. Information System Owner (ISO)

The ISO:

- Tests, validates, and documents changes to the information system before implementing the changes on the operational system. Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in security control [CM-6](#).
- Ensures potential security impacts are analyzed prior to the implementation of information systems or changes to information systems, and if implemented, that impacts are documented in the system's security documentation (e.g., System Security Plan).

2.7. Impact Analysis (CM-4)

2.7.1. Information System Owner (ISO)

The ISO:

- Analyzes changes to the information system to determine potential security or privacy impacts prior to change implementation.
- Ensures that a security impact analysis/privacy impact analysis is conducted.
- Ensures the security impact analysis/privacy impact analysis includes reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls.
- Ensures the assessment of risk documents impact of changes and provides additional controls if required.

2.8. Access Restrictions for Change (CM-5)

2.8.1. Information System Owner (ISO)

The ISO:

- Manages individuals' logical and physical access privileges to change information systems in a manner consistent with ODVs.

- Defines, documents, approves, and enforces logical and physical access restrictions to making changes to information systems in the system's security documentation (e.g., System Security Plan), in a manner consistent with ODVs.

2.9. Configuration Settings (CM-6)

2.9.1. Cybersecurity Standards and Engineering Team

The Cybersecurity Standards and Engineering Team:

- CSET establishes and documents configuration settings for IT products employed within information systems. If a specification does not exist for an information system, Information Security Owners shall use the Risk-Informed Decision-making process in [NPR 8000.4, Agency Risk Management Procedural Requirements](#). The ISO shall then reference and implement specific Center guidance or guidance from the one of the following sources, in declining order of authority
 - Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
 - National Security Agency (NSA) Configuration Guides
 - NIST-produced checklists for civilian agency use
 - Center for Internet Security (CIS) Benchmarks

2.10. Configuration Settings | Automated Management, Application, and Verification (CM-6(1))

2.10.1. Office of the Chief Information Officer (OCIO)

The OCIO:

- Provides the Continuous Diagnostics and Monitoring (CDM) Hardware Asset Management/Software Asset Management (HWAM/SWAM) solution to centrally manage, apply (for some systems), and verify configuration settings for information systems and components, as applicable.

2.10.2. Information System Owner (ISO)

The ISO:

- Employs the CDM HWAM/SWAM solution where possible.
- If use of the CDM HWAM/SWAM solution is not possible, the ISO will document a waiver or risk-based decision in accordance with Agency requirements, and will employ automated mechanisms to manage, apply, and verify configuration settings for their system.

2.11. Least Functionality (CM-7)

2.11.1. Information System Owner (ISO)

The ISO:

- Configures the information system to:
 - Provide only capabilities essential to the system's mission and business function.

- Prohibit or restrict the use of the following function, ports, protocols, and/or services: File Transfers and peer-to-peer.

2.12. Least Functionality I Periodic Review (CM-7(1))

2.12.1. Information System Owner (ISO) and/or Information System Security Officer (ISSO)

The ISO and/or ISSO:

- Reviews the information system at least quarterly to:
 - Identify functions, ports, protocols, and services that are non-secure and/or not necessary to the system's mission and business function.
 - Disable or remove functions, ports, protocols, and services that are non-secure and/or not necessary to the system's mission and business function.

2.13. Least Functionality I Prevent Program Execution (CM-7(2))

2.13.1. Information System Owner (ISO)

The ISO:

- Ensures that the information system prevents program execution in accordance with NASA policies regarding software program usage and restrictions.

2.14. Least Functionality I Unauthorized Software/ Allow by Exception (CM-7(5))

2.14.1. Information System Owner (ISO) and/or Information System Security Officer (ISSO)

The ISO and/or ISSO:

- Identifies and continuously monitors and manages software programs authorized to execute on the information system.
- Employs a deny-by-default, permit-by-exception policy to disallow the execution of unauthorized software programs on the information system.

2.15. Information System Component Inventory (CM-8)

2.15.1. Office of the Chief Information Officer (OCIO)

The OCIO:

- Provides the CDM HWAM/SWAM solution to develop and document an accurate inventory of all information system components within the authorization boundary of the system at an appropriate level of granularity. Specific information collected can be viewed in IT Security-Enterprise Data Warehouse (ITSEC-EDW).
- The CDM HWAM/SWAM solution inventories system components once per week.

2.15.2. Information System Owner (ISO)

The ISO:

- Utilizes the CDM HWAM/SWAM solution to inventory system components.
- If it is not possible to utilize the CDM HWAM/SWAM solution, the ISO will document a waiver or risk based decision in accordance with Agency requirements, and will develop and document an accurate inventory of all information system components within the authorization boundary at an appropriate level of granularity using the NASA Manual Inventory.
- The ISO will review and update the information system component inventory at least once per quarter.
- Verifies that no components within the authorization boundary of the information system are duplicated in other information system inventories.

2.16. Information System Component inventory I Updates During Installations/Removals (CM-8(1))

2.16.1. Office of the Chief Information Officer (OCIO)

The OCIO:

- Provides the CDM HWAM/SWAM solution which, in some cases, automatically collects inventory of information system components upon installation, removal, and updates. If inventory is not updated upon installation, removal, or update, the inventory is updated as part of its scheduled weekly inventory update.

2.16.2. Information System Owner (ISO)

The ISO:

- Utilizes the CDM HWAM/SWAM solution.
- If it is not possible to utilize the CDM HWAM/SWAM solution, the ISO will document a waiver or risk-based decision in accordance with Agency requirements, and is responsible for updating system component inventories upon installation, removal, and update.

2.17. Information System Component Inventory | Automated Maintenance (CM-8(2))

2.17.1. Office of the Chief Information Officer (OCIO)

The OCIO:

- Provides a CDM HWAM/SWAM solution as an automated mechanism to maintain an up-to-date, complete, accurate and readily available inventory of information system component

2.17.2. Information System Owner (ISO)

The ISO:

- Utilizes the CDM HWAM/SWAM solution.
- If it is not possible to utilize the CDM HWAM/SWAM solution, the ISO will document a waiver or risk based decision in accordance with Agency requirements, and is responsible for employing automated mechanisms to help

maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

2.18. Information System Component Inventory I Automated Unauthorized Component Detection (CM-8(3))

2.18.1. Office of the Chief Information Officer (OCIO)

The OCIO:

- Provides the CDM HWAM/SWAM solution as an automated mechanism to maintain an up-to-date, complete, accurate and readily available inventory of information system components.
- Provides the enterprise Network Access Control (NAC) capability to detect and alert on the connection of unauthorized hardware components.

2.18.2. Information System Owner (ISO)

The ISO:

- Utilizes the CDM HWAM/SWAM solution information (or, if unable to utilize the CDM HWAM/SWAM solution, documents the waiver or risk based decision as appropriate, and employs another mechanism) to monitor hardware components within the information system
- Employs automated mechanisms to detect the presence of unauthorized software and firmware components within the information system and notifies the SOC upon discovery.

2.18.3. Information System Owner (ISO) and/or Center Chief Information Security Officer (Center CISO)

The ISO and/or Center CISO:

- Takes the following actions when unauthorized components are detected: disable network access by such components, isolates the components, and notify 1550, Contracting Officer Representative (COR), ISO, and the NASA SOC.

2.19. Configuration Management Plan (CM-9)

2.19.1. Information System Owner (ISO)

The ISO:

- Documents and implements a Configuration Management Plan that includes:
- Roles, responsibilities, and processes and procedures for configuration management of the information system.
- Configuration items for the information system and when in the development life cycle the configuration items are placed under configuration management.
- A means for identifying configuration items and the processes for those items' control and management.
- Key management stakeholders responsible for reviewing and approving proposed changes to the information system.
- Personnel responsible for conducting security impact analysis of information systems and changes to the system.

2.20. Software Usage Restrictions (CM-10)

2.20.1. Enterprise License Management Team

The Enterprise License Management Team:

- Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution.

2.20.2. Information System Owner (ISO)

The ISO:

- Ensures the use of NASA Software Inventory system which allows for tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution in accordance with contract agreements and copyright laws.
- Employs NASA Software Inventory whitelisting solution to enforce any Agency or Center/organizational issued white/black software lists.
- Controls and documents any use of peer-to-peer file sharing technology as a component of information system operation to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work, or in other restricted content scenarios (e.g., Sensitive but Unclassified).

2.21. User-Installed Software (CM-11)

2.21.1. Senior Agency Information Security Officer (SAISO)

The SAISO:

- Establishes approved and non-approved/restricted software lists governing the installation of software by users.

2.21.2. Information System Owner (ISO)

The ISO:

- Enforces software installation policies through Agency software tools.

2.21.3. Information System Security Officer (ISSO)

The ISSO:

- Monitors policy compliance quarterly.

2.21.4. NASA User

The NASA User:

- Complies with NASA policy and rules of behavior prohibiting the installation of unauthorized software by users.

APPENDIX A: ACRONYMS

ASCS	Agency Security Configuration Standards
CDM	Continuous Diagnostics and Monitoring
CIC	Chief Information Officer
CIS	Center for Internet Security
CENTER CISO	Center Chief Information Security Officer
COR	Contracting Officer Representative
CSET	Cybersecurity Standards and Engineering Team
CSPD	Cybersecurity and Privacy Division
EDW	Enterprise Data Warehouse
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
HBK	Handbook
HWAM	Hardware Asset Management
IMS	Incident Management System
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
ITSEC-EDW	IT Security Enterprise Data Warehouse
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
RISCS	Risk Information Security Compliance System
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center

SP	Special Publication
SWAM	Software Asset Management

[1] Refer to the ISO responsibilities under this control: the ISO sets the conditions for NASA SOC to detect and report IT security incidents.