NISTIR 8011
Volume 2

Automation Support for Security Control Assessments

Volume 2: Hardware Asset Management

Kelley Dempsey
Paul Eavy
George Moore

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8011-2

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8011
Volume 2

Automation Support for Security Control Assessments

Volume 2: Hardware Asset Management

Kelley Dempsey
Computer Security Division
Information Technology Laboratory

Paul Eavy
Federal Network Resilience Division
Department of Homeland Security

George Moore
Johns Hopkins University
Applied Physics Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8011-2

June 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8011, Volume 2
155 pages (June 2017)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8011-2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST information security publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal systems.

Abstract

The NISTIR 8011 volumes focus on each individual information security capability, adding tangible detail to the more general overview given in NISTIR 8011 Volume 1, and providing a template for transition to a detailed, NIST standards-compliant automated assessment. This document, Volume 2 of NISTIR 8011, addresses the Hardware Asset Management (HWAM) information security capability. The focus of the HWAM capability is to manage risk created by unmanaged and/or unauthorized devices on a network. Unmanaged devices are targets that attackers can use to gain and more easily maintain a persistent platform from which to attack the rest of the network.

Keywords

actual state; assessment; assessment boundary; assessment method; authorization boundary; automated assessment; automation; capability; continuous diagnostics and mitigation; dashboard; defect; defect check; desired state specification; hardware asset management; information security continuous monitoring; inventory management; mitigation; ongoing assessment; root cause analysis; security automation; security capability; security control; security control assessment; security control item.

Acknowledgments

The authors, Kelley Dempsey of the National Institute of Standards and Technology (NIST), Dr. George Moore of the Applied Physics Laboratory at Johns Hopkins University, and Paul Eavy of the Department of Homeland Security, wish to thank their colleagues who reviewed drafts of this document, including Nathan Aileo, Nadya Bartol, Craig Chase, Ann Dixon, Terry Fletcher, Jim Foti, John Groenveld, Susan Hansche, Alicia Jones, Amy Heydman, Elizabeth Lennon, Jaime Miller, Susan Pagan, Daniel Portwood, Ron Ross, Martin Stanley, Kevin Stine, Robin Walker, David Waltermire, Kimberly Watson, and Jim Wiggins**.** The authors also gratefully acknowledge and appreciate the comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

Table of Contents

List of Figures

List of Tables

Executive Summary

The National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) have collaborated on the development of a process that automates the test assessment method described in NIST Special Publication (SP) 800-53A for the security controls catalogued in SP 800-53. The process is consistent with the Risk Management Framework as described in SP 800-37 and the Information Security Continuous Monitoring (ISCM) guidance in SP 800-137. The multi-volume NIST Interagency Report 8011 (NISTIR 8011) has been developed to provide information on automation support for ongoing assessments. NISTIR 8011 describes how ISCM facilitates automated ongoing assessment to provide near-real-time security-related information to organizational officials on the security posture of individual systems and the organization as a whole.

NISTIR 8011 Volume 1 includes a description of *ISCM Security Capabilities*—groups of security controls working together to achieve a common purpose. The subsequent NISTIR 8011 volumes are capability-specific volumes. Each volume focuses on one specific ISCM information security capability in order to (a) add tangible detail to the more general overview given in NISTIR 8011 Volume 1; and (b) provide a template for the transition to detailed, standards-compliant automated assessments.

This document, Volume 2 of NISTIR 8011, addresses the information security capability known as Hardware Asset Management (HWAM). The focus of the HWAM capability is to manage risk created by unmanaged or unauthorized devices that are on a network. When devices are unmanaged or unauthorized, they are vulnerable because the devices tend to be forgotten or unseen. Moreover, when vulnerabilities are discovered on such devices, there is no one assigned to respond to the risk. As a result, unmanaged and unauthorized devices are targets that attackers can use to gain and more easily maintain a persistent platform from which to attack the rest of the network.

A well-designed HWAM program helps to prevent (a) entry of exploits or natural events into a network; (b) exploits or events from gaining a foothold; and (c) the exfiltration of information. The assessment helps verify that hardware asset management is working.

This volume outlines detailed step-by-step processes to adapt or customize the template presented here to meet the needs of a specific assessment target network and apply the results to the assessment of all authorization boundaries on that network. A process is also provided to implement the assessment (diagnosis) and response. Automated testing related to the controls for HWAM, as outlined herein, is compliant with other NIST guidance.

It has not been obvious to security professionals how to automate testing of other than technical controls. This volume documents a detailed assessment plan to assess the effectiveness of controls related to authorizing and assigning devices to be managed. Included are specific tests that form the basis for such a plan, how the tests apply to specific controls, and the kinds of resources needed to operate and use the assessment to mitigate defects found. For HWAM, it can

be shown that the assessment of 88 percent[1] of determination statements for controls in the SP 800-53 Low-Medium-High baselines can be fully or partially automated.

The methods outlined here are designed to provide objective, timely, and complete identification of security defects related to HWAM at a lower cost than manual assessment methods. Using this defect information can drive the most efficient and effective remediation of the worst security defects found.

This volume assumes the reader is familiar with the concepts and ideas presented in the Overview (NISTIR 8011, Volume 1). Terms used herein are also defined in the Volume 1 glossary.

[1] Derived from the Control Allocation Tables (CAT) in this volume. With respect to security controls selected in the SP 800-53 Low-Medium-High baselines that support the HWAM capability, 38 of 43 determination statements (88%) can be fully or partially automated.

1. Introduction

1.1 Purpose and Scope

The purpose of the National Institute of Standards (NIST) Interagency Report (NISTIR) 8011 Volume 2 is to provide an operational approach for automating the assessment of SP 800-53 security controls related to the ISCM-defined security capability of *Hardware Asset Management* (HWAM) that is consistent with the principles outlined in Volume 1.

The scope is limited to security controls/control items that are implemented for **hardware**.

1.2 Target Audience

The target audience for this volume, because it is focused on HWAM, is of special relevance to those who manage hardware. However, it is still of value to others to help understand the risks hardware may be imposing on non-hardware assets.

1.3 Organization of this Volume

Section 2 provides an overview of the HWAM capability to clarify both scope and purpose and provides links to additional information specific to the HWAM capability. Section 3 provides detailed information on the HWAM defect checks and how the defect checks automate assessment of the effectiveness of SP 800-53 security controls that support the HWAM capability. Section 3 also provides artifacts that can be used by an organization to produce an automated security control assessment plan for most of the control items supporting Hardware Asset Management.

1.4 Interaction with Other Volumes in this NISTIR

Volume 1 of this NISTIR (Overview) provides a conceptual synopsis of using automation to support security control assessment and provides definitions and background information that facilitates understanding of the information in this and subsequent volumes. This volume assumes that the reader is familiar with the information in Volume 1.

The HWAM capability identifies devices (defined in Figure 2) that are present on the target network and supports other capabilities by providing the full census of devices on which to check for defects related to software, device privileges, and device behavior.

2. Hardware Asset Management (HWAM) Capability Definition, Overview, and Scope

Hardware asset management recognizes that networked devices that are unauthorized[2] and/or unassigned for management are likely to be vulnerable. External and inside attackers search for and exploit such devices, either for what the device itself can offer, or as a platform from which to persist on the network to attack other assets. By removing unauthorized devices and/or assigning such devices to a person or team for system administration and authorization, HWAM helps reduce the probability that attackers find and easily exploit devices.

2.1 HWAM Capability Description

The Hardware Asset Management Capability provides an organization visibility into the devices operating on its network(s), so it can manage and defend itself in an appropriate manner. It also provides a view of device management responsibility in a way that prioritized defects can be presented to the responsible party for mitigation actions and risk acceptance decisions.

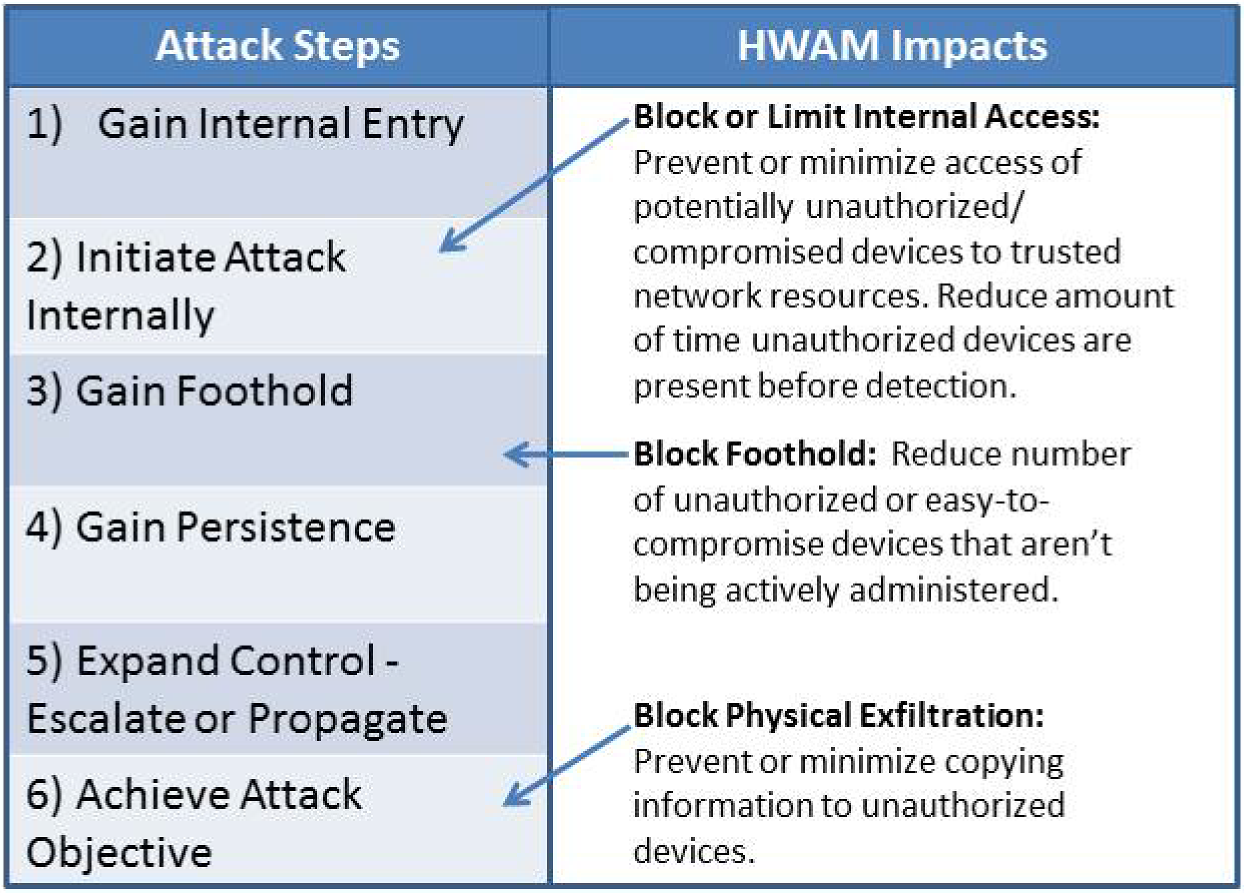
HWAM identifies devices, including virtual machines, that are present on the network and compares them with the *desired state* inventory to determine if the devices identified as being on the target network are authorized. Some devices are network-addressable, and others are removable (and presumably connected to addressable devices). The HWAM capability is focused on ensuring that all devices authorized to be on the target network are fully identified and that an appropriate access control policy is applied, thus the means for identifying the actual devices will vary, depending on the automated tools in use and the type of device.

The ISCM process (as adapted for each agency) provides insight into what percentage of the actual hardware assets are included in the desired state, and of those, how many identify an assigned manager.

2.2 HWAM Attack Scenarios and Desired Result

This document (NISTIR 8011) uses an attack step model to summarize the seven primary steps of cyber attacks that SP 800-53 controls work together to block or delay (see Figure 1: HWAM Impact on an Attack Step Model). The HWAM security capability is designed to block or delay attacks at the attack steps listed in Table 1: HWAM Impact on an Attack Step Model.

[2] Unauthorized devices are those devices that have not been assessed and authorized to operate as part of an overall system authorization process or individually if the device was added to a system after the initial system authorization.



Attack Steps

1) Gain Internal Entry

2) Initiate Attack Internally

3) Gain Foothold

4) Gain Persistence

5) Expand Control - Escalate or Propagate

6) Achieve Attack Objective

HWAM Impacts

Block or Limit Internal Access: Prevent or minimize access of potentially unauthorized/ compromised devices to trusted network resources. Reduce amount of time unauthorized devices are present before detection.

Block Foothold: Reduce number of unauthorized or easy-to-compromise devices that aren't being actively administered.

Block Physical Exfiltration: Prevent or minimize copying information to unauthorized devices.

Figure 1: HWAM Impact on an Attack Step Model

Note

The attack steps shown in Figure 1: HWAM Impact on an Attack Step Model, apply only to adversarial attacks. (See NISTIR 8011, Volume 1, Section 3.2.)

Table 1: HWAM Impact on an Attack Step Model

Attack Step Name	Attack Step Purpose	Examples of HWAM Impact
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Block or Limit Internal Access: Prevent or minimize access of potentially unauthorized/compromised devices to trusted network resources; Reduce amount of time unauthorized devices are present before detection.

Attack Step Name	Attack Step Purpose	Examples of HWAM Impact
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Block Foothold: Reduce number of unauthorized and/or easy-to-compromise devices that aren't being actively administered.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Block Physical Exfiltration: Prevent or minimize copying information to unauthorized devices.

Other examples of traceability among requirement levels. While Table 1 shows HWAM impacts on example attack steps, it is frequently useful to observe traceability among other sets of requirements. To examine such traceability, see Table 2: Traceability among Requirement Levels. To reveal traceability from one requirement type to another, look up the cell in the matching row and column of interest and click on the link.

Table 2: Traceability among Requirement Levels

	Example Attack Steps	Capability	Sub-Capability/ Defect Check	Control Items
Example Attack Steps		Figure 1 Table 1	Table 6	Appendix A
Capability	Figure 1 Table 1		Table 6	Section 3.3[a]
Sub-Capability/ Defect Check	Table 6	Table 6		Section 3.2[b]
Control Items	Appendix A	Section 3.3[a]	Section 3.2[b]	

[a] Each level-four section (e.g., 3.3.1.1) is a control item that supports this capability.

[b] Refer to the table under the heading *Supporting Control Items* within each defect check.

2.3 Assessment Objects Protected and Assessed by HWAM

As noted in Section 1.1, the assessment objects directly managed and assessed by the HWAM capability are hardware devices. However, the following clarification is relevant:

Hardware that cannot be attacked independently is not included in the definition of a device (Figure 2: Definition of *Devices* for HWAM). For example, remote attacks affect a device through its Internet Protocol (IP) connection and cannot attack a mouse independently. Thus, subcomponents of the device (Figure 3: Definition of *Device Subcomponents* for HWAM) are important primarily if they can be moved or accessed as independent devices (e.g., a thumb drive) or they impose risk to the overall device or the network (e.g., a wireless capability). These considerations drive the selected definitions. Otherwise, for HWAM purposes, items like a mouse, monitor, or internal memory are simply parts of the device.

Devices (hardware assets), which are defined in the HWAM architecture and Concept of Operations [Figure 4 and HWAM Capability Description], consist of the following:

- IP addressable (or otherwise network addressable) physical hardware; and
- IP addressable virtual devices.

Note: In NIST SP 800-53, revision 4, Section 1.1, footnote 9, devices make up almost all examples of “system components.” Therefore, devices are considered to be system components.

Figure 2: Definition of *Devices* for HWAM

Subcomponents are the parts or functionalities which make up a device. Organizations may ***optionally*** choose to track subcomponents and their attributes if they carry security implications. Device subcomponents ***may*** include, but are not limited to:

- modem connections;
- wireless capabilities;
- hardware that is not IP addressable (e.g., some network switches); and
- removable hardware of security interest
    - USB thumb drives;
    - removable hard drives; and
    - other removable media.

Individual organizations have a great deal of flexibility in defining device subcomponents as needed to meet organization specific needs. Thus, no precise definition of subcomponents is provided.

Figure 3: Definition of *Device Subcomponents* for HWAM

2.4 Example HWAM Data Requirements[3]

Examples of data requirements for the HWAM actual state are in Table 3. Examples of data requirements for the HWAM desired state are in Table 4.

Table 3: Example HWAM Actual State Data Requirements

Data Item	Justification
Data necessary to accurately identify the device. Site-specific, examples include: • IP Address; • Media Access Control (MAC) Address; • Host-based certificate or applicable Agent ID(s); • Device domain name; • Device authentication with means such as 802.1x AR..	To identify which operational device is unauthorized, or has some other defect.
Data necessary to describe the attributes of a device such that other capabilities can determine the appropriate defect checks to run on that device.[a] • Software identification (SWID) tag or Common Platform Enumeration (CPE) for operating system of device or equivalent: ▪ Vendor; ▪ Product; ▪ Version; ▪ Release level; and ▪ Patch level.	To ensure all appropriate defects for devices are defined, executed, and reported.
Data necessary to compare devices connected to the network to the authorized hardware inventory. • IP Address; • MAC Address; • Host-based certificate or Agent ID; • Device domain name; and • Machine-readable hardware identifiers.	To identify unauthorized devices.
Data necessary to locate physical assets based on information collected in the operational environment. Site specific, examples include: • Edge switch that detected device; and • Hosts to which USB drive was connected.	To ensure that specific locations of devices are known so devices can be found to repair, validate, or remove if needed.
Data necessary to determine how long devices have been present in the environment. At a minimum: • Date/time it was first discovered; and • Date/time it was last seen.	To determine how long the device has been in existence and the last time it was detected in the enterprise

[a] This information could also be collected by SWAM tools (see Volume 3).

[3] Specific data required is variable based on organizational platforms, tools, configurations, etc.

Table 4: Example HWAM Desired State Data Requirements

Data Item	Justification
Data necessary to accurately identify the device. At a minimum: • Serial Number or vendor asset tag; • Expected CPE for hardware or equivalent: ▪ Vendor; ▪ Product; ▪ Model Number; • Static IP Address (where applicable); • MAC Address; and • Property Number. Local enhancements[a] might include data necessary to accurately identify device sub-components.	To uniquely identify the device. To validate that the device on the network is the device authorized, and not an imposter.
Data necessary to describe a device such that other capabilities can determine the appropriate defect checks to run on that device. • Expected SWID tag or CPE for operating system of device or equivalent: ▪ Vendor; ▪ Product; ▪ Version; ▪ Release level; and ▪ Patch level.	To ensure all appropriate defects for a device are defined, run, and reported. To help identify non-reporting associated with other capabilities that look for defects on the device.
A person or organization that is the device manager for each device (note: this should be a reasonable assignment, do not count management assignments where a person or organization is assigned too many devices to effectively manage the devices). Local enhancements might include: • Approvers being assigned; • Managers being approved; and • Managers acknowledging receipt.	To identify the role responsible for responding to specific risk conditions found. To assess the performance of the response roles in risk management.

Data Item	Justification
Data necessary to compare devices discovered on the network to the authorized hardware inventory. Site dependent, examples include: • IP address; • MAC address; • Host-based certificate or Agent ID; and • Device domain name.	To identify unauthorized devices. To know which devices have defects.
Data necessary to locate a physical device. • Expected connection points (e.g., switch port, wireless access point), if any; and • Expected physical location (e.g., building number, room number)..	To ensure that managers can find the device to revalidate it for supply chain risk management. • Remove it if unauthorized
The period of time the device is authorized. Local enhancements might include: • When the device must be physically inspected/verified for supply chain risk management	To allow previously authorized devices to remain in the authorized hardware inventory, but know such devices are no longer authorized.
Expected status of the device (e.g., authorized, expired, pending approval, missing) to include: • Date first authorized; • Date of most recent authorization; and • Date authorization revoked. Local enhancements might include: • Returned from high-risk location; • Removed pending reauthorization; and • Date of last status change.	To determine which devices in the authorized hardware inventory are not likely to be found in actual state inventory.

[a] Organizations can define data requirements and associated defects for their local environment.

2.5 HWAM Concept of Operational Implementation

Figure 4: HWAM Concept of Operations (CONOPS) illustrates how HWAM might be implemented. The CONOPS is central to the automated assessment process.

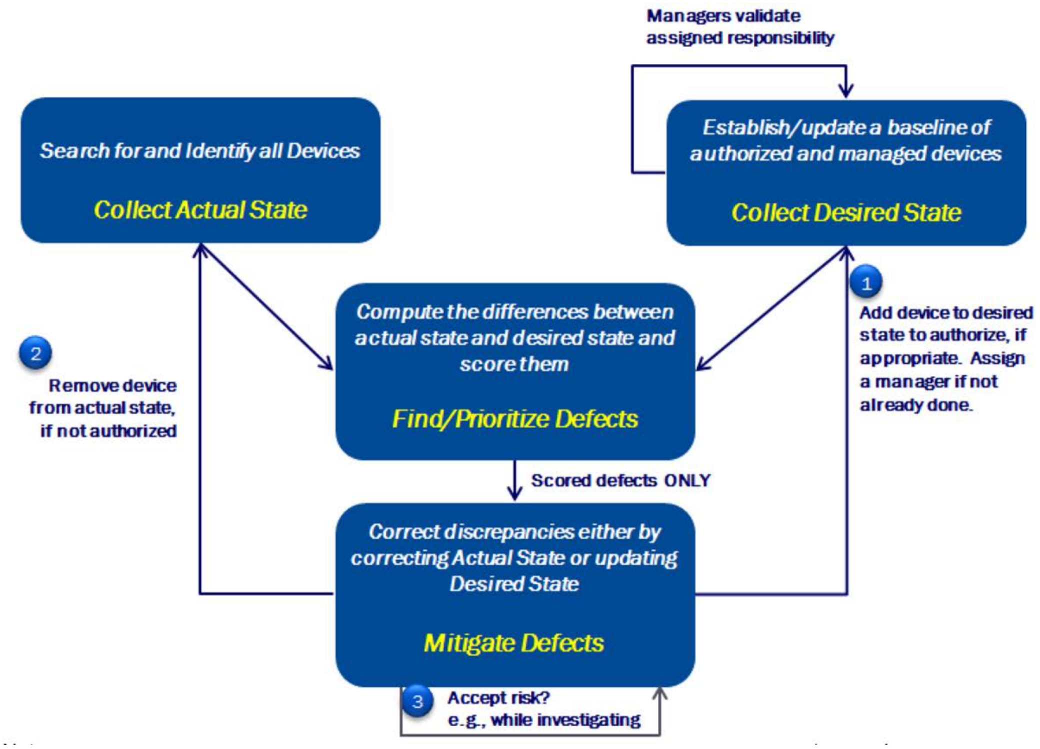

Managers validate assigned responsibility
Search for and Identify all Devices
Collect Actual State
Establish/update a baseline of authorized and managed devices
Collect Desired State
1
Add device to desired state to authorize, if appropriate. Assign a manager if not already done.
2
Remove device from actual state, if not authorized
Compute the differences between actual state and desired state and score them
Find/Prioritize Defects
Scored defects ONLY
Correct discrepancies either by correcting Actual State or updating Desired State
Mitigate Defects
3
Accept risk? e.g., while investigating

Figure 4: HWAM Concept of Operations (CONOPS)

The following is a brief description of the HWAM capability functionality:

> HWAM identifies devices (including virtual machines) that are present on the network (the actual state) and compares them with the desired state inventory to determine if the identified devices are authorized for operation and connection to the network. Some devices are IP-addressable (or equivalent), and others are organization-defined device subcomponents connected through addressable devices). The means for identifying the actual devices will vary, depending on the automated capabilities available and which type of device it is.

2.5.1 Collect Actual State

Use tools to collect information about what IP-addressable devices, virtual machines and removable media are present on the network. The network and connected devices are continuously observed to detect and learn about IP-addressable devices and removable media. Methods to detect devices (when it was first seen, and when/where it was last seen) may include (but are not limited to):

- Passive listening to identify devices talking;
- Active IP range scanning, to detect devices (e.g., respond to a "ping");
- Active mining of Dynamic Host Configuration Protocol (DHCP) logs and/or switch tables; and
- Network Access Control (if present).

Methods to learn about discovered devices may include (but are not limited to):

- Passive listening to types of traffic to/from devices;
- Active methods (e.g., trace route) to collect data about the device's location; and
- Active agents on the device to detect organization-defined subcomponents and other details.

The ISCM data collection process identifies the devices that are on the network that are addressable and can provide the information required to compare the devices with the authorized inventory. Also, it is necessary to identify how much of the network is being monitored to discover the actual hardware operating on it. Device authentication significantly improves the quality of actual state data.

2.5.2 Collect Desired State

Create an Authorized Hardware Inventory using policies, procedures, and processes suggested by the information security program or as otherwise defined by the organization. Expected output is a hardware inventory that contains identifying information for a device, when it was authorized, when the authorization expires, who manages the device and the removable media authorized for each device.

2.5.3 Find/Prioritize Defects

Comparing the list of devices discovered on the network (actual state) with the authorized hardware inventory list (desired state) often reveals that devices exist on one list and not on the other. The comparison identifies both unauthorized devices and missing authorized devices that may indicate a security risk. Additional defects related to hardware management may be defined by the organization. After the comparison is complete, identified defects are scored and prioritized[4] (using federal- and organization-defined criteria) so that the appropriate response action can be taken (i.e., higher risk problems are addressed first).

2.6 SP 800-53 Control Items that Support HWAM

This section documents how control items that support HWAM were identified as well as the nomenclature used to clarify each control item's focus on hardware.

2.6.1 Process for Identifying Needed Controls

A section on Tracing Security Control Items to Capabilities explains the process used to determine the controls needed to support a capability—this process is described in detail in Volume 1 of this NISTIR. In short, the two steps are:

[4] A risk scoring methodology is necessary to score and prioritize defects but risk scoring is out of scope for this publication.

1. Use a keyword search of the control text to identify control items that might support the capability. See keyword rules in Appendix B.
2. Manually identify those that *do* support the capability (true positives) and ignore those that do not (false positives).

This produces three sets of controls:

1. The control items in the low, moderate, and high baselines that support the HWAM capability (listed in the section on HWAM Control (Item) Security Assessment Plan Narrative Tables and Templates and the section on Control Allocation Tables).
2. Control items in the low, moderate, and high baselines that were selected by the keyword search, but were manually determined to be false positives (listed in Appendix C).
3. Control items which were not in a baseline, and not analyzed further after the keyword search. These include:
    a. The Program Management Family of controls, because those controls do not apply to individual systems.
    b. The *not selected* controls—controls that are in SP 800-53 but are not assigned to (selected in) a baseline.
    c. The Privacy Controls.

    The unanalyzed controls are listed in Appendix D, in case the organization wants to develop automated tests.

2.6.2 Control Item Nomenclature

Many control items that support the HWAM capability also support several other capabilities. For example, hardware, software products, software settings, and software patches may all benefit from configuration management controls.

To add clarity to the scope of such control items related to HWAM, the parenthetic expression {hardware} is included in this volume to denote that a particular control item, as it supports the HWAM capability, focuses on—and only on—hardware.

2.7 HWAM Specific Roles and Responsibilities

Table 5: Operational and Managerial Roles for HWAM, describes HWAM-specific roles and the corresponding responsibilities. Figure 5: Primary Roles in Automated Assessment of HWAM, shows how the roles integrate with the concept of operations. An organization implementing automated assessment can customize its approach by assigning (allocating) the responsibilities to persons in existing roles.

Table 5: Operational and Managerial Roles for HWAM

Role Code	Role Title	Role Description	Role Type
DM	Device Manager (DM)	Assigned to a specific device or group of devices, device managers are (for HWAM) responsible for adding/removing devices from the network, and for configuring the hardware of each device (adding and removing hardware components). The device managers are specified in the desired state inventory specification. The device manager may be a person or a group. If a group, there is a group manager in charge.	Operational
DSM	Desired State Managers and Authorizers (DSM)	Desired State Managers are needed for both the ISCM Target Network and each assessment object. The desired state managers ensure that data specifying the desired state of the relevant capability is entered into the ISCM system's desired state data and is available to guide the actual state collection subsystem and to identify defects. The DSM for the ISCM Target Network also resolves any ambiguity about which system authorization boundary has defects (if any). Authorizers share some of the responsibilities by authorizing specific items (e.g., devices, software products, or settings), and thus defining the desired state. The desired state manager oversees and organizes this activity.	Operational
ISCM-Ops	ISCM Operators (ISCM-OPS)	ISCM operators are responsible for operating the ISCM system (see ISCM-Sys).	Operational
ISCM-Sys	The system that collects, analyzes and displays ISCM security-related information	The ISCM system: a) collects the desired state specification; b) collects security-related information from sensors (e.g., scanners, agents, training applications, etc.); and c) processes that information into a useful form. To support task c) the system conducts specified defect check(s) and sends defect information to an ISCM dashboard covering the relevant system(s). The ISCM system is responsible for the assessment of most SP 800-53 security controls.	Operational
MAN	Manual Assessors	Assessments not automated by the ISCM system are conducted by human assessors using manual/procedural methods. Manual/procedural assessments might also be conducted to verify the automated security-related information collected by the ISCM system—when there is a concern about data quality.	Operational
RskEx	Risk Executive, System Owner, and/or Authorizing Official (RskEx)	Defined in SPs 800-37 and 800-39.	Managerial
TBD	To be determined by the organization	Depends on specific use. TBD by the organization.	Unknown

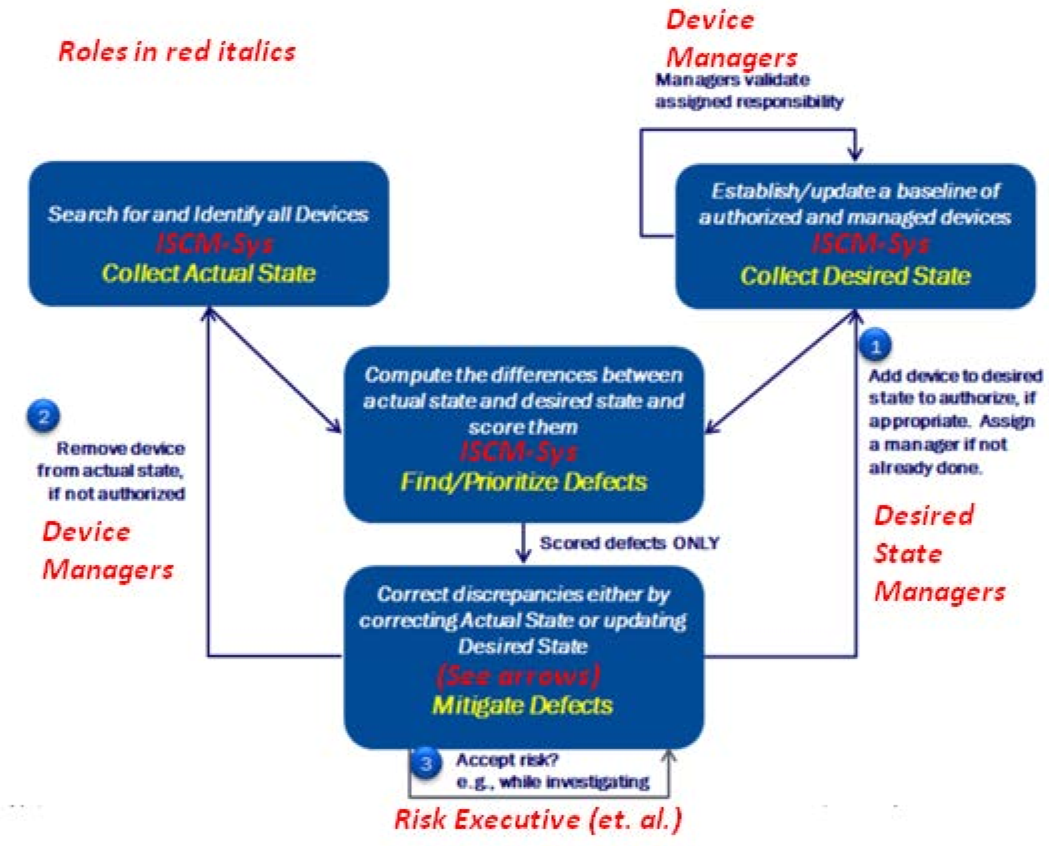

Roles in red italics
Device
Managers
Managers validate assigned responsibility
Search for and Identify all Devices
ISCM-Sys
Collect Actual State
Establish/update a baseline of authorized and managed devices
ISCM-Sys
Collect Desired State
1
Add device to desired state to authorize, if appropriate. Assign a manager if not already done.
2
Remove device from actual state, if not authorized
Device
Managers
Compute the differences between actual state and desired state and score them
ISCM-Sys
Find/Prioritize Defects
Scored defects ONLY
Desired
State
Managers
Correct discrepancies either by correcting Actual State or updating Desired State
(See arrows)
Mitigate Defects
3
Accept risk? e.g., while investigating
Risk Executive (et. al.)

Figure 5: Primary Roles in Automated Assessment of HWAM

2.8 HWAM Assessment Boundary

The assessment boundary is ideally an entire *network* of computers from the innermost enclave out to where the network either ends in an air-gap or interconnects to other network(s)—typically the Internet or the network(s) of a partner or partners. For HWAM, the boundary includes all devices inside this boundary and associated components, including removable devices. For more detail and definitions of some the terms applicable to the assessment boundary, see Section 4.3.2 in Volume 1 of this NISTIR.

Some consideration must be given to cloud environments used, but not operated, by the organization. In this environment, the virtual machines (VMs) used are inside the HWAM, as are the communication paths to access them. The physical hardware on which the VMs operate and other devices on the cloud may be considered outside the assessment boundary if they are isolated from the VMs used, but not otherwise.

2.9 HWAM Actual State and Desired State Specification

For information on the actual state and the desired state specification for HWAM, see the assessment criteria notes section of the defect check tables in Section 3.2.

Note that many controls in HWAM refer to developing and updating an inventory of devices (or other inventories). Note also, that per the SP 800-53A definition of *test*, testing of the HWAM controls implies the need for specification of both an actual state inventory and a desired state inventory, so that the test can compare the two inventories. The details of this are described in the defect check tables in Section 3.2.

2.10 HWAM Authorization Boundary and Inheritance

See Section 4.3.1 of Volume 1 of this NISTIR for information on how authorization boundaries are handled in automated assessments. In short, for HWAM, each device is assigned to one and only one authorization (system) boundary, per SP 800-53 CM-08(5), System Component Inventory | No Duplicate Accounting of Components. The ISCM dashboard can include a mechanism for recording the assignment of devices to authorization boundaries, making sure all devices are assigned to at least one such boundary, and that no device is assigned to more than one boundary.

For information on how inheritance is managed, see Section 4.3.3 of Volume 1 of this NISTIR. For HWAM, many network devices [e.g., firewalls, Lightweight Directory Access Protocols (LDAPs)] provide inheritable controls for other systems. The ISCM dashboard can include a mechanism to record such inheritance and use it in assessing the system's overall risk.

2.11 HWAM Assessment Criteria Recommended Scores and Risk-Acceptance Thresholds

General guidance on options for using risk scores to set risk-acceptance thresholds is outside the scope of this NISTIR. In any case, organizations performing HWAM are encouraged to use metrics that look at both average risk and maximum risk per device.

2.12 HWAM Assessment Criteria Device Groupings to Consider

To support automated assessment and ongoing authorization, devices need to be clearly grouped by authorization boundary [see Control Items CM-8a and CM-8(5) in SP 800-53] and by the device managers responsible for specific devices [see Control Item CM-8(4) in SP 800-53]. In addition to these two important groupings, the organization may want to use other groupings for risk analysis, as discussed in Section 5.6 of Volume 1 of this NISTIR.

3. HWAM Security Assessment Plan Documentation Template

3.1 Introduction and Steps for Adapting This Plan

This section provides templates for the security assessment plan in accordance with SP 800-37 and SP 800-53A. The documentation elements used are described in Section 6 of Volume 1 of this NISTIR. Section 9 of Volume 1 specifically describes how the templates and documentation relate to the assessment tasks and work products defined in SP 800-37 and SP 800-53A. The following are suggested steps to adapt this plan to the organization's needs and implement automated monitoring.

Figure 6 shows the main steps in the adoption process. The steps are expanded to more detail in the following three sections.

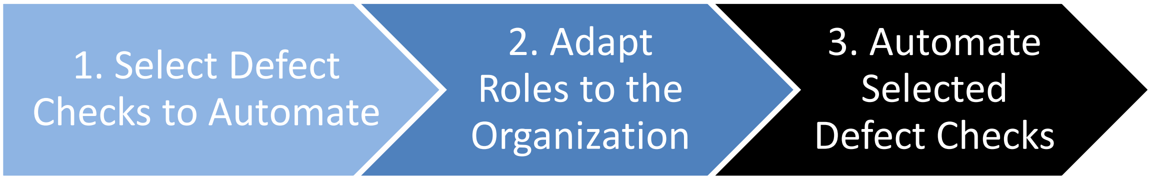

1. Select Defect Checks to Automate
2. Adapt Roles to the Organization
3. Automate Selected Defect Checks

Figure 6: Main Steps in Adapting the Plan Template

3.1.1 Select Defect Checks to Automate

The main steps in selecting local defect checks to automate are described in this section.

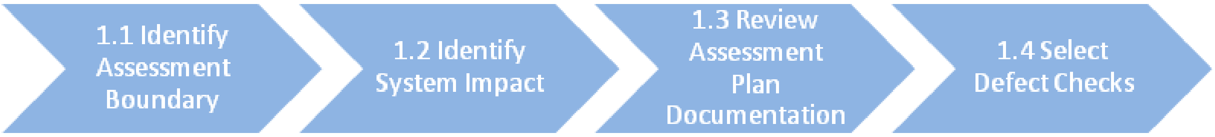

1.1 Identify Assessment Boundary
1.2 Identify System Impact
1.3 Review Assessment Plan Documentation
1.4 Select Defect Checks

Figure 7: Sub-Steps to Select Defect Checks to Automate

Take the following steps to select which local defect checks to automate:

(1) **Identify Assessment Boundary:** Identify the assessment boundary to be covered. (See Section 4.3 of Volume 1 of this NISTIR.)

(2) **Identify System Impact:** Identify the Federal Information Processing Standard (FIPS) 199-defined impact level for that assessment boundary.
(See SP 800-60 and/or organizational categorization records.)

(3) **Review Security Assessment Plan Documentation:**

a. Review the defect checks documented in Section 3.2 to get an initial sense of the proposed items to be tested.

b. Review the security assessment plan narratives in Section 3.2 to understand how the defect checks apply to the controls that support hardware asset management.

(4) **Select Defect Checks:**

a. Based on Steps (2) to (4) in this list and an understanding of the organization’s risk tolerance, use Table 6: Mapping of Attack Steps to Security Sub-Capability, in Section 3.2.3 to identify the local defect checks that would be necessary to test controls required by the impact level and risk tolerance.

b. Mark the local defect checks necessary as selected in Section 3.2.2. The organization is not required to use automation, but automation of testing adds value to the extent that it:

(i) Produces assessment results timely enough to better defend against attacks; and/or

(ii) Reduces the cost of assessment over the long term.

3.1.2 Adapt Roles to the Organization

The main steps to adapt the roles to the organization are described in this section.

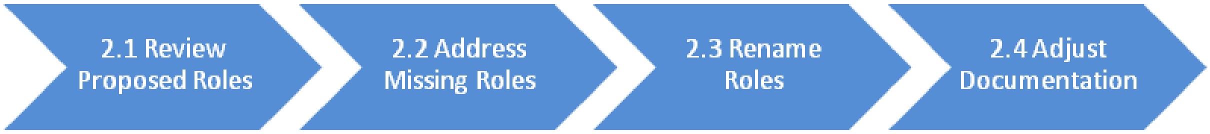


Figure 8: Sub-Steps to Adapt Roles to the Organization

(1) **Review Proposed Roles**: Proposed roles are described in Section 2.7, HWAM Specific Roles and Responsibilities (Illustrative).

(2) **Address Missing Roles:** Identify any required roles not currently assigned in the organization. Determine how to assign the unassigned roles.

(3) **Rename Roles:** Identify the organization-specific names that match each role. (Note that more than one proposed role might be performed by the same organizational role.)

(4) **Adjust Documentation:** Map the organization-specific roles to the roles proposed herein, in one of two ways (either may be acceptable):

a. Add a column to the table in Section 2.7 for the organization-specific role and list it there; or

b. Use global replace to change the role names throughout the documentation from the names proposed here to the organization-specific names.

3.1.3 Automate Selected Defect Checks

The main steps to implement automation are described in this section.

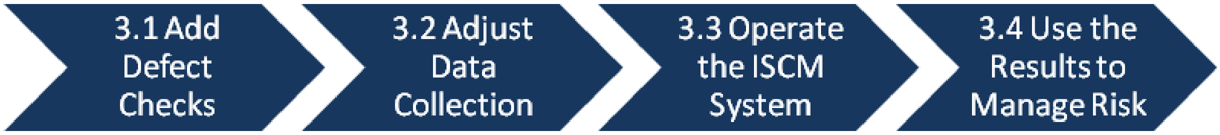

3.1 Add Defect Checks
3.2 Adjust Data Collection
3.3 Operate the ISCM System
3.4 Use the Results to Manage Risk

Figure 9: Sub-Steps to Automate Selected Defect Checks

(1) **Add Defect Checks:** Review the defect check definition and add checks as needed based on organizational risk tolerance and expected attack types. [Role: DSM (See Section 2.7.)]

(2) **Adjust Data Collection:**

a. Review the actual state information needed and configure automated sensors to collect the required information. [Role: ISCM-Sys (See Section 2.7.)]

b. Review the matching desired state specification that was specified or add additional specifications to match the added actual state to be checked. Configure the collection system to receive and store this desired state specification in a form that can be automatically compared to the actual state data. [Role: ISCM-Sys (See Section 2.7.)]

(3) **Operate the ISCM-System:**

a. Operate the collection system to identify both security and data quality defects.

b. Configure the collection system to send security and data quality information to the defect management dashboard.

(4) **Use the Results to Manage Risk:** Use the results to respond to the problems that will reduce risk most significantly first (given the impact and/or effort involved in correction) and to measure potential residual risk to inform aggregate risk acceptance decisions. If risk is determined to be too great for acceptance, the results may also be used to help prioritize further mitigation actions.

3.2 HWAM Sub-Capabilities and Defect Check Tables and Templates

This section documents the specific test templates that are proposed and considered adequate to assess the control items that support HWAM. See Section 5 of Volume 1 of this NISTIR for an overview of defect checks, and see Section 4.1 of Volume 1 for an overview of the actual state and desired state specifications discussed in the Assessment Criteria Notes for each defect check. Sections 3.2.1 and 3.2.2 of this document describe the foundational and local defect checks, respectively. The *Supporting Control Item(s)* data in sections 3.2.1 and 3.2.2 document which controls might cause any of the checks to fail, i.e., documenting why the check (test) might be needed. Refer to Section 3.1 on how to adapt the defect checks (and roles specified therein) to the organization.

Data found in Section 3.2 can be used in both defect check selection and root cause analysis, as described there. Section 3.2.3 documents how each sub-capability (tested by a defect check) serves to support the overall capability by addressing certain example attack steps and/or data quality issues.

The Defect Check Templates are organized around four-part tables, as follows:

(1) Part 1 of the table is preceded by the text, “The purpose of this sub-capability is defined as follows:” and contains the following columns:

a. **Sub-Capability Name**.

b. **Sub-Capability Purpose**. This is a description of the sub-capability purpose. Note that *how* sub-capabilities block or delay attack steps is described in Section 3.2.3.)

(2) Part 2 of the table is preceded by the text, “The defect check to assess whether this sub-capability is operating effectively is defined as follows:” and contains the following columns:

a. **Defect Check ID**. Defect check identifier.

b. **Defect Check Name**.

c. **Assessment Criteria Summary**. Short description of what is checked.

d. **Assessment Criteria Notes**. Used to assess whether or not the sub-capability is effective in achieving its purpose.

(3) Part 3 of the table describes potential responses and example roles for taking response actions. It begins with a paragraph that leads with the words, “**Example Responses**.” Following the paragraph are three columns of the table:

a. **Defect Check ID**. Defect check identifier. This is identical to the defect check identifier of Part 2.

b. **Potential Response Action**. Examples of responses that might be appropriate when the check finds a defect and what role is likely responsible.

c. **Primary Responsibility**. The person or role that might appropriately respond to the defect found.

d. **Selected**. Yes or No, indicating if this defect check is selected for assessment.

(4) Part 4, the last part of the table, lists the SP 800-53 control items that work together to support this sub-capability. It begins with a paragraph that leads with the words, "**Supporting Control Items**," and is followed by the remainder of the paragraph, and then the four columns described below. Identification of supporting control items is based on the mapping of defect checks to control items described in Section 3.3.

a. **Defect Check ID**. Defect check identifier. This is identical to the defect check identifier of Part 2 and Part 3.

b. **Baseline**. Low, Moderate, or High.

c. **Sortable Control Item Code**. The Sortable Control Item Code is used to manage and sort security control items within a database. The Sortable Control Item Code is always accompanied by its corresponding SP 800-53 Control Item Code (next column). See the NISTIR 8011 Volume 1 glossary for definition of Sortable Control Item Code.

d. **SP-800-53 Control Item Code**.

As noted in Section 3.1, this material is designed to be customized and adapted to become part of an organization's security assessment plan.

3.2.1 Foundational Sub-Capabilities and Corresponding Defect Checks

This document (NISTIR 8011) proposes two foundational security-oriented defect checks for the HWAM capability. The foundational checks are designated HWAM-F01 and HWAM-F02 and focus on security.

Four *data quality* defect checks are also proposed and are designated HWAM-Q01 through HWAM-Q04. The data quality defect checks are important because they provide the information necessary to document how reliable the overall assessment automation process is, information which can be used to decide how much to trust the other data (i.e., provide greater assurance about security control effectiveness). Defect checks may be computed for individual checks (e.g., federal and/or local), or summarized for various groupings of devices (e.g., device manager, device owner, system, etc.) out to the full assessment boundary.

Each of the foundational and data quality defect checks is defined in terms of assessment criteria, mitigation methods, and responsibility described in the *Example Mitigation/Responses* section under each defect check.

The foundational and data quality defect checks were selected for their value for summary reporting. The *Selected* column indicates which of the checks to implement.

3.2.1.1 Prevent Unauthorized Devices *Sub-Capability and Defect Check HWAM-F01*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Prevent unauthorized devices	Prevent or reduce the presence of unauthorized devices, thus reducing the number of potentially malicious or high-risk devices.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID		Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-F01		Unauthorized devices	Device is present in the assessment boundary (*is* in Actual State) but has not been authorized to be there (is *not* in Desired State) [See supplemental criteria in L02]	Assessment Criteria Notes: 1) The actual state is the list (inventory) of all devices (within an organizationally defined tolerance) in the assessment boundary as determined by the ISCM system. 2) The desired state specification is a list of all devices authorized to be in the assessment boundary. 3) A defect is a device in the actual state but not in the desired state, and is thus unauthorized. This is computed by simple set differencing.	Yes

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-F01	Remove Device	DM
HWAM-F01	Authorize Device	DSM
HWAM-F01	Accept Risk	RskEx
HWAM-F01	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code[a]	SP 800-53 Control Item Code
HWAM-F01	Low	AC-19-b	AC-19(b)
HWAM-F01	Low	CM-08-a	CM-8(a)
HWAM-F01	Low	CM-08-b	CM-8(b)
HWAM-F01	Low	PS-04-d	PS-4(d)
HWAM-F01	Low	SC-15-a	SC-15(a)
HWAM-F01	Moderate	AC-20-z-02-z	AC-20(2)
HWAM-F01	Moderate	CM-03-b	CM-3(b)
HWAM-F01	Moderate	CM-03-c	CM-3(c)
HWAM-F01	Moderate	CM-03-d	CM-3(d)
HWAM-F01	Moderate	CM-03-g	CM-3(g)
HWAM-F01	Moderate	CM-08-z-01-z	CM-8(1)
HWAM-F01	Moderate	CM-08-z-03-b	CM-8(3)(b)
HWAM-F01	Moderate	MA-03-z-01-z	MA-3(1)
HWAM-F01	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-F01	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-F01	High	CM-03-z-01-d	CM-3(1)(d)

[a] The Sortable Control Item Code is used to manage and sort security control items within a database. The Sortable Control Item Code is always shown with the associated SP 800-53 Control Item Code. See Volume 1 glossary for definition of *Sortable Control Item Code*.

3.2.1.2 Reduce Number of Devices without Assigned Device Manager *Sub-Capability and Defect Check HWAM-F02*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce number of devices without assigned device manager	Prevent or reduce the number of authorized devices without an assigned device manager within the assessment boundary, thus reducing delay in mitigating device defects (when found).

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-F02	Authorized devices without a device manager	Device is in Actual State and in Desired State (both from HWAM-F01) but no approved device manager is assigned.	Assessment Criteria Notes: 1) The actual state is the list of device managers assigned to manage each device plus a list of approved device managers as determined by the ISCM system. 2) The desired state specification is that a device manager is specified for each device, and is in the list of approved device managers. 3) A defect is an authorized device in the HWAM-F01 actual state where the device manager is either not listed or listed but not on the approved list. Such devices are called devices without an assigned device manager". Note: The HWAM-F01 status must be known to assess HWAM-F02. Also note that an unmanaged device that has never been on the network (in the HWAM-F1 Actual State) is not counted as a defect because it cannot cause risk to the network until it is on the network. The organization still needs to consider risk to the system(s) from the unconnected device(s), if any, but because it is outside the assessment boundary, the ISCM assessment cannot do this.	Yes

Example Mitigation/Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-F02	Remove Device	DM
HWAM-F02	Assign Device	DSM
HWAM-F02	Accept Risk	RskEx
HWAM-F02	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-F02	Low	AC-19-b	AC-19(b)
HWAM-F02	Low	CM-08-z-04-z	CM-8(4)
HWAM-F02	Moderate	CM-03-b	CM-3(b)
HWAM-F02	Moderate	CM-03-c	CM-3(c)
HWAM-F02	Moderate	CM-03-d	CM-3(d)
HWAM-F02	Moderate	CM-03-g	CM-3(g)
HWAM-F02	Moderate	MA-03-z-01-z	MA-3(1)
HWAM-F02	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-F02	High	CM-03-z-01-b	CM-3(1)(b)

3.2.1.3 Ensure Reporting of Devices *Sub-Capability and Defect Check HWAM-Q01*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure reporting of devices	Ensure that individual devices are regularly reported in the actual state inventory to prevent defects associated with other capabilities from going undetected.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-Q01	Non-reporting devices	Device in Desired State but not reported, as recently as expected, to be in Actual State.	Assessment Criteria Notes: 1) The actual state is the same as HWAM-F01. 2) The desired state is the same as HWAM-F01. 3) A defect occurs when a device in the desired state has not been detected as recently as expected in the actual state. Criteria are developed to define the threshold for “as recently as expected,” for each device or device type based on the following considerations: a. some devices (e.g., domain controllers, routers) must always be present. b. devices may not report in a particular collection because the devices are turned off, network connections are temporarily down, etc. But the devices should appear in the actual state at least every *n* collections, where “*n*” is defined by “as recently as expected.” c. defining “as recently as expected” for devices such as laptops might require information on what percent of the time the devices are expected to be connected to the network and powered on. As that percent goes down, the length of “as recently as expected” would go up. Time and experience are required to accurately define “as recently as expected” for each device/device type in order to eliminate false positives while still finding true positives.	Yes

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-Q01	Restore Device Reporting	ISCM-Ops
HWAM-Q01	Declare Device Missing	DM
HWAM-Q01	Accept Risk	RskEx
HWAM-Q01	Ensure Correct Response	ISCM-Ops

Supporting Control Items: This sub-capability is supported by each of the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-Q01	Low	CM-08-a	CM-8(a)
HWAM-Q01	Moderate	CM-03-f	CM-3(f)
HWAM-Q01	Moderate	CM-03-z-02-z	CM-3(2)
HWAM-Q01	Moderate	CM-08-z-01-z	CM-8(1)
HWAM-Q01	High	CM-08-z-02-z	CM-8(2)

3.2.1.4 Ensure Reporting of Defect Checks *Sub-Capability and Defect Check HWAM-Q02*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure reporting of defect checks	Ensure that defect check information is reported in the actual state inventory to prevent systematic inability to check any defect on any device.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-Q02	Non-reporting defect checks	Defect Checks are selected, but the HWAM Actual State Collection Manager does not report testing for all defects on all devices. (Device level and defect check level defect.)	Assessment Criteria Notes: 1) The actual state is the set of HWAM data that was collected in each collection cycle to support all implemented HWAM defect checks. 2) The desired state is the set of HWAM data that must be collected in each collection cycle to support all implemented HWAM defect checks. 3) The defect is any set of data needed for a defect where not all the data was collected for a specified number of devices (too many devices) indicating that the collection system is not providing enough information to perform a complete assessment. Criteria are developed to define the threshold for “too many devices” in order to balance the need for completeness with the reality that some data may be missing from even the highest quality collections.	Yes

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST documents. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-Q02	Restore Defect Check Reporting	ISCM-Ops
HWAM-Q02	Accept Risk	RskEx
HWAM-Q02	Ensure Correct Response	ISCM-Ops

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-Q02	Low	CM-08-a	CM-8(a)
HWAM-Q02	Moderate	CM-03-f	CM-3(f)
HWAM-Q02	Moderate	CM-03-z-02-z	CM-3(2)

3.2.1.5 Ensure Defect Check Completeness *Sub-Capability and Defect Check HWAM-Q03*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure defect check completeness	Ensure that data for as many defect checks as possible are correctly reported in the actual state inventory to prevent defects from persisting undetected across the assessment boundary.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-Q03	Low completeness metric	Completeness of the actual inventory collection is below an [organization-defined-threshold]. (Summary of Q03 and Q04 for assessment boundary and other device grouping (e.g., system, device manager, etc.))	Assessment Criteria Notes: Unlike Q01 and Q02, the completeness metric is not a device-level or defect-check-level defect, but is applied to any collection of devices – for example, those in a system authorization boundary. It is used in computing the overall maturity of the collection system. 1) The actual state is the number of specified defect checks provided by the collection system in a reporting window. 2) The desired state is the number of specified defect checks that should have been provided in that same reporting window. 3) Completeness is the actual state number divided by the desired state number – that is, it is the percentage of specified defect checks collected during the reporting window. Completeness measures long term ability to collect all needed data. 4) The metric is completeness, defined as the actual state number divided by the desired state number. 5) A defect is when completeness is too low (based on the defined threshold). This indicates risk because, when completeness is too low, there is too much risk of defects being undetected. An acceptable level of completeness balances technical feasibility against the need for 100% completeness. Note on 1): A specific check-device combination may only be counted once in the required minimum reporting period. For example, if checks are to be done every 3 days, a check done twice in that timeframe would still count as 1 check. However, if there are 30 days in the reporting window, that check-	Yes

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
			device combination could be counted for each of the ten 3-day periods included. Note on 2): Different devices may have different sets of specified checks, based on the device role. The desired state in this example includes ten instances of each specified defect-check combinations for each of the 3-day reporting cycles in a 30-day reporting window.	

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-Q03	Restore Completeness	ISCM-Ops
HWAM-Q03	Accept Risk	RskEx
HWAM-Q03	Ensure Correct Response	ISCM-Ops

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-Q03	Low	CM-08-a	CM-8(a)
HWAM-Q03	Moderate	CM-03-f	CM-3(f)
HWAM-Q03	Moderate	CM-03-z-02-z	CM-3(2)
HWAM-Q03	High	CM-08-z-02-z	CM-8(2)

3.2.1.6 Ensure Reporting Timeliness *Sub-Capability and Defect Check HWAM-Q04*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure reporting timeliness	Ensure that data for as many defect checks as possible are reported in a timely manner in the actual state inventory to prevent defects from persisting undetected. To be effective, defects need to be found and mitigated considerably faster than the defects can be exploited.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-Q04	Poor timeliness metric	Frequency of update (timeliness) of the actual inventory collection is lower than an [organization-defined-threshold]. (Summary of Q03 and Q04 for assessment boundary and other device grouping (e.g., system, device manager, etc.)	Assessment Criteria Notes: Unlike Q01 and Q02, the Timeliness metric is not a device-level or defect-check-level defect, but can be applied to any collection of devices – for example, those within a system (authorization boundary). It is used in computing the overall maturity of the collection system. 1) The actual state is the number of specified defect checks provided by the collection system in one collection cycle – the period in which each defect should be checked once. 2) The desired state is the number of specified defect checks that should have been provided in the collection cycle. 3) Timeliness is the actual state number divided by the desired state number – that is, it is the percentage of specified defect checks collected in the reporting cycle. Thus it measures the percentage of data that is currently timely (collected as recently as required). 4) The metric is timeliness, defined as the actual state number divided by the desired state number. 5) A defect is when “timeliness” is too poor (based on the defined threshold). This indicates risk because when timeliness is poor there is too much risk of defects not being detected quickly enough. Note on 1): A specific check-device combination may only be counted once in the collection cycle. Note on 2): Different devices may have different sets of specified checks, based on the device role.	Yes

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST documents. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-Q04	Restore Frequency	ISCM-Ops
HWAM-Q04	Accept Risk	RskEx
HWAM-Q04	Ensure Correct Response	ISCM-Ops

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-Q04	Low	CM-08-a	CM-8(a)
HWAM-Q04	Low	CM-08-b	CM-8(b)
HWAM-Q04	Moderate	CM-03-f	CM-3(f)
HWAM-Q04	Moderate	CM-03-g	CM-3(g)
HWAM-Q04	Moderate	CM-03-z-02-z	CM-3(2)
HWAM-Q04	Moderate	CM-08-z-01-z	CM-8(1)
HWAM-Q04	Moderate	CM-08-z-03-a	CM-8(3)(a)
HWAM-Q04	High	CM-08-z-02-z	CM-8(2)

3.2.2 Local Sub-Capabilities and Corresponding Defect Checks

This section includes local defect checks, as examples of what organizations may add to the foundational checks to support more complete automated assessment of SP 800-53 controls that support HWAM.

Organizations exercise authority to manage risk by choosing whether or not to select specific defect checks for implementation. In general, selecting more defect checks may lower risk (if there is capacity to address defects found) and provide greater assurance but may also increase cost of detection and mitigation. The organization selects defect checks for implementation (or not) to balance the benefits and costs and prioritize risk response actions by focusing first on the problems that pose greater risk (i.e., manage risk).

Note that each local defect check may also include options to make it more or less rigorous, as the risk tolerance of the organization deems appropriate.

The “Selected” column is present to indicate which of the checks the organization chooses to implement as documented or as modified by the organization.

3.2.2.1 Reduce Exploitation of Devices before Removal, during Use Elsewhere, and after Return *Sub-Capability and Defect Check HWAM-L01*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce exploitation of devices before removal, during use elsewhere, and after return	Prevent exploitation of devices before removal, during use elsewhere, and after return (or other mobile use) by a) appropriately hardening the device prior to removal from protected spaces; b) checking for organizational data before removal from protected spaces; and c) sanitizing the device before introduction or reintroduction into the assessment boundary.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L01	Devices moving into/out of the assessment boundary	The desired state is that the device is approved for removal and connection. The device type or sub-components do not meet organization defined rules (for removal and/or connection).	Assessment Criteria Notes: 1) The actual state includes four parts: a. the actual hardware configuration of devices approved for removal. The hardware configuration typically consists of the presence or absence of specific hardware subcomponents (e.g., DVD drives, USB ports). b. data identifying devices about to be used in travel (and to where). c. users authorized to take the devices on travel. d. data identifying devices reentering the assessment boundary (and where else the device has been connected while removed - this might be validated from GPS and IP logging, if appropriate). 2) The desired state includes two parts: a. the list of devices authorized for removal; and b. the desired hardware configuration and/or sanitization for such devices, based on connections while removed. [Reference 1a and 1d, above.] 3) A defect occurs when: a. any device unauthorized for removal is either expected to be (or has actually been) removed, regardless of hardware configuration. b. a device approved for travel does not have the desired hardware configuration for the proposed uses. c. a device approved for travel was connected to unapproved location(s) where its hardware configuration was not appropriate (matching the desired state) for those location(s).	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L01	Remove Authorization for Travel	DM
HWAM-L01	Correct the hardware configuration	DM
HWAM-L01	Accept Risk	RskEx
HWAM-L01	Ensure Correct Response	DM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L01	Low	AC-19-a	AC-19(a)
HWAM-L01	Low	PS-04-d	PS-4(d)
HWAM-L01	Low	SC-15-a	SC-15(a)
HWAM-L01	Moderate	AC-20-z-02-z	AC-20(2)
HWAM-L01	Moderate	CM-02-z-07-a	CM-2(7)(a)
HWAM-L01	Moderate	CM-02-z-07-b	CM-2(7)(b)
HWAM-L01	Moderate	CM-03-b	CM-3(b)
HWAM-L01	Moderate	CM-03-c	CM-3(c)
HWAM-L01	Moderate	CM-03-d	CM-3(d)
HWAM-L01	Moderate	CM-03-g	CM-3(g)
HWAM-L01	Moderate	MA-03-z-01-z	MA-3(1)
HWAM-L01	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L01	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-L01	High	MA-03-z-03-a	MA-3(3)(a)
HWAM-L01	High	MA-03-z-03-b	MA-3(3)(b)

3.2.2.2 Reduce Insider Threat of Unauthorized Device *Sub-Capability and Defect Check HWAM-L02*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce insider threat of unauthorized device	Require multiple persons to authorize adding a device to the authorization boundary (i.e., apply the principle of separation of duties) to limit the ability of a single careless or malicious insider to authorize devices. Note 1: The organization might choose to use access restrictions to enforce the separation of duties. If so, that would be assessed under the PRIV capability. What is assessed here is that the separation of duties occurs. Note 2: See HWAM-L11 for authorization boundary.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L02	Required authorization missing	Device is connected before being approved by at least two authorized persons.	Assessment Criteria Notes: 1) The actual state is the list of persons who authorized the change to the system, thus allowing the device to be connected inside the assessment boundary. This would typically be recorded in the desired state inventory as part of the configuration change control process. 2) The desired state is the list of persons who are authorized to approve system changes and allow devices to be connected inside the assessment boundary. This may include rules to support separation of duties specifying first, second, etc., approver roles. 3) A defect occurs when: a. addition of the device is authorized by less than the required number of distinct and authorized approvers; or b. addition of the device is authorized by persons not authorized to approve changes to the system (at each step in the approval process).	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L02	Remove Device	DM
HWAM-L02	Authorize Device	DSM
HWAM-L02	Accept Risk	RskEx
HWAM-L02	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L02	Moderate	CM-03-b	CM-3(b)
HWAM-L02	Moderate	CM-03-c	CM-3(c)
HWAM-L02	Moderate	CM-03-d	CM-3(d)
HWAM-L02	Moderate	CM-03-g	CM-3(g)
HWAM-L02	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L02	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-L02	High	CM-03-z-01-d	CM-3(1)(d)

3.2.2.3 Reduce Denial of Service Attacks from Missing Required Devices/Subcomponents *Sub-Capability and Defect Check HWAM-L03*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce denial of service attacks resulting from missing required devices and/or device subcomponents.	Prevent or reduce denial of service attacks and/or attacks on resilience by ensuring that all required devices and organization-defined subcomponents are present in the assessment boundary.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L03	Required device and/or device subcomponent not installed	Device and/or device subcomponent is in the desired state and is authorized, but has not appeared in the actual state after [an organization-defined] number of collections.	Assessment Criteria Notes: 1) The actual state is the same as for HWAM-F01, the inventory of devices and/or device subcomponents actually found to be connected inside the assessment boundary. 2) The desired state includes: a. a supplement to the desired state for HWAM-F01 that specifies that some devices and/or device subcomponents are not only authorized, but required to be present on the network; and b. a time frame and frequency of search for determining that the absence of the device and/or device subcomponent is not a false positive. For example, this might specify that if the device/subcomponent is absent after an active search conducted every x minutes, the device/subcomponent is considered absent. 3) A defect occurs when a device and/or device subcomponent is listed as required in the desired state, but has not been identified in the actual state within the number of checks (n) within the specified frequency (x).	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L03	Install Device	DM
HWAM-L03	Remove Requirement	DSM
HWAM-L03	Accept Risk	RskEx
HWAM-L03	Ensure Correct Response	DM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L03	Low	CM-08-a	CM-8(a)
HWAM-L03	Moderate	AC-20-z-02-z	AC-20(2)
HWAM-L03	Moderate	CM-03-b	CM-3(b)
HWAM-L03	Moderate	CM-03-c	CM-3(c)
HWAM-L03	Moderate	CM-03-d	CM-3(d)
HWAM-L03	Moderate	CM-03-g	CM-3(g)
HWAM-L03	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L03	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-L03	High	CM-03-z-01-f	CM-3(1)(f)
HWAM-L03	High	MA-03-z-03-a	MA-3(3)(a)
HWAM-L03	High	MA-03-z-03-b	MA-3(3)(b)

3.2.2.4 Restrict Device Ownership *Sub-Capability and Defect Check HWAM-L04*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Restrict Device Ownership	Ensure that devices not owned by the organization are not connected in the assessment boundary, or that the devices are authorized for connection only in accordance with organizationally defined restrictions.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L04	Restrictions on device ownership	The device is not owned by the organization or is not in compliance with defined restrictions for non-organizationally owned device connection.	Assessment Criteria Notes: This check is relevant where connection of non-organizationally owned devices in the assessment boundary is allowed. The assessment criteria provided here include examples, and could be expanded to include other criteria of interest to the organization. 1) The actual state includes: a. the same inventory as for HWAM-F01, the inventory of devices actually found to be connected inside the assessment boundary. b. identifiers associated with defined restrictions for non-organizationally owned devices (e.g., connection type/limits, specific persons or roles permitted to connect such devices). c. the length of time (or period) each device has been connected. d. IP or MAC address of the connected non-organizationally owned device. 2) The desired state includes: a. a list of approved device owners or roles. b. a list of authorized devices approved for connection by each owner. c. rules to determine limits to connection time or periods. d. other organization-defined identifiers associated with defined restrictions for non-organizationally owned devices. 3) A defect occurs when: a. a device with no owner or an owner not on the approved owner list for that device is connected. b. a device is connected which violates restrictions on length or time of connection. c. a device without the required identifiers is connected. d. a device fails other organizationally defined restrictions related to connection of non-organizationally owned devices.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L04	Remove Device	DM
HWAM-L04	Authorize Owner	DSM
HWAM-L04	Accept Risk	RskEx
HWAM-L04	Ensure Correct Response	DM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L04	Moderate	AC-19-z-05-z	AC-19(5)
HWAM-L04	Moderate	CM-03-b	CM-3(b)
HWAM-L04	Moderate	CM-03-c	CM-3(c)
HWAM-L04	Moderate	CM-03-d	CM-3(d)
HWAM-L04	Moderate	CM-03-g	CM-3(g)
HWAM-L04	Moderate	MP-07-z-01-z	MP-7(1)
HWAM-L04	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L04	High	CM-03-z-01-b	CM-3(1)(b)

3.2.2.5 Reduce Unapproved Suppliers and/or Manufacturers *Sub-Capability and Defect Check HWAM-L05*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce unapproved suppliers and/or manufacturers	Prevent or reduce supply chain threats in devices (e.g., by ensuring that all authorized devices are from trusted suppliers and/or manufacturers).

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L05	Unapproved supplier and/or manufacturer	The device supplier and/or manufacturer is not on an approved list. Note: The organization could design other ways to establish supply chain trust.	Assessment Criteria Notes: 1) The actual state includes: a. the HWAM-F01 actual state inventory; b. the device manufacturer, based on inventory data about the device; and c. the device supplier, typically recorded during the device's authorization in the desired state inventory. 2) The desired state includes: a. a list of trusted manufacturers; and b. a list of trusted suppliers 3) A defect occurs when: a. a device is in the actual state inventory without an authorized manufacturer; b. a device is in the actual state inventory without an authorized supplier; c. a device is in the desired state inventory without an authorized manufacturer; and/or d. a device is in the desired state inventory without an authorized supplier. Note: While the actual state for a device is static, the desired state can change, typically causing a defect when a provider becomes untrusted.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L05	Remove Device	DM
HWAM-L05	Correct the Supplier Data	DSM
HWAM-L05	Correct the Manufacturer Data	ISCM-OPS
HWAM-L05	Accept Risk	RskEx
HWAM-L05	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L05	Moderate	CM-03-b	CM-3(b)
HWAM-L05	Moderate	CM-03-c	CM-3(c)
HWAM-L05	Moderate	CM-03-d	CM-3(d)
HWAM-L05	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L05	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-L05	High	SA-12	SA-12

3.2.2.6 Reduce Unauthorized Device Subcomponents *Sub-Capability and Defect Check HWAM-L06*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Reduce unauthorized device subcomponents	Detect and remove unauthorized device subcomponents to implement least functionality in order to prevent or reduce the introduction of device subcomponents that could enable attacks.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L06	Device sub-components not authorized	Device has unauthorized hardware device subcomponents.	Assessment Criteria Notes: 1) The actual state includes the list of actual hardware subcomponents discovered on a device. 2) The desired state includes the list of authorized device subcomponents: a. by device role/attributes; or b. by device identity. 3) A defect occurs when a device actually in the assessment boundary has unauthorized hardware device subcomponents.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L06	Remove Device Subcomponent	DM
HWAM-L06	Authorize Device Subcomponent	DSM
HWAM-L06	Accept Risk	RskEx
HWAM-L06	Ensure Correct Response	DM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item
HWAM-L06	Low	AC-19-a	AC-19(a)
HWAM-L06	Low	CM-08-a	CM-8(a)
HWAM-L06	Moderate	AC-19-z-05-z	AC-19(5)
HWAM-L06	Moderate	CM-03-b	CM-3(b)
HWAM-L06	Moderate	CM-03-c	CM-3(c)
HWAM-L06	Moderate	CM-03-d	CM-3(d)
HWAM-L06	Moderate	CM-03-g	CM-3(g)
HWAM-L06	Moderate	CM-08-z-03-b	CM-8(3)(b)
HWAM-L06	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L06	High	CM-03-z-01-b	CM-3(1)(b)

3.2.2.7 Verify Ongoing Business Need for Device *Sub-Capability and Defect Check HWAM-L07*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Verify ongoing business need for device	Require periodic and/or event driven consideration of whether a device is still needed for system functionality to fulfill mission requirements in support of least functionality. Note: Good practice dictates that DMs review managed devices and System Owners review device functionality required within the authorization boundary as well as identifying non-supportable/end-of-life devices in a timely manner.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L07	Business need and/or device manager not recently verified	Device has expired sunset date.	Assessment Criteria Notes: 1) The actual state includes (for each device): a. the current date; and/or b. whether or not a specified trigger event has occurred. 2) The desired state includes: a. the maximum time before re-verification is required for each device; b. a device sunset date; and c. specific events requiring consideration of device relevance: i. by device role/attributes; and/or ii. by device identity. 3) A defect occurs when a device that is present in the assessment boundary: a. has an expired sunset date; b. is nearing an expired sunset date (to provide warning to desired state managers); and/or c. a specified trigger event has occurred to this device without re-verification of business need.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L07	Remove Device	DM
HWAM-L07	Re-authorize Device	DSM
HWAM-L07	Accept Risk	RskEx
HWAM-L07	Ensure Correct Response	DM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L07	Moderate	CM-03-b	CM-3(b)
HWAM-L07	Moderate	CM-03-c	CM-3(c)
HWAM-L07	Moderate	CM-03-d	CM-3(d)
HWAM-L07	Moderate	CM-03-f	CM-3(f)
HWAM-L07	Moderate	CM-03-g	CM-3(g)
HWAM-L07	Moderate	CM-08-z-01-z	CM-8(1)
HWAM-L07	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L07	High	CM-03-z-01-b	CM-3(1)(b)

3.2.2.8 Ensure Required Device Data is Collected *Sub-Capability and Defect Check HWAM-L08*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure required device data is collected	Ensure that data required to assess risk are collected. Such data may relate to other than a HWAM defect but may need to be generated by the HWAM collector. For example, devices with inadequate memory to support basic OS as well as defensive security devices may need to be identified during collection so such problems can be detected as defects.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L08	Missing required device data	Required device data not collected within required time frame.	Assessment Criteria Notes: 1) The actual state includes: a. the list of data attributes collected on each device by the actual state collection system; and b. the date each attribute was last collected. 2) The desired state includes: a. the list of attributes that are required to be collected for each device, specified: i. by device role/attributes; and/or ii. by device identity; and b. the time frame within which each attribute should be collected based on the same role/attribute/identity. 3) A defect occurs when the required data has not been collected from a device within the required time frame.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L08	Remove Non-reporting Devices	DM
HWAM-L08	Begin to Collect All Required Data	ISCM-OPS
HWAM-L08	Change Reporting Requirements	RskEx
HWAM-L08	Accept Risk	RskEx
HWAM-L08	Ensure Correct Response	ISCM-OPS

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L08	Low	CM-08-a	CM-8(a)
HWAM-L08	Low	CM-08-b	CM-8(b)

3.2.2.9 Ensure Needed Changes Are Approved or Disapproved in a Timely Manner *Sub-Capability and Defect Check HWAM-L09*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure needed changes are approved or disapproved in a timely manner	Ensure that needed changes are approved or disapproved in a timely manner by flagging requested changes not considered (approved or disapproved) in a timely manner as risks.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L09	Proposed changes are too old	Proposed changes not approved or disapproved after [organization-defined time frame]. Assumes L02 is selected.	Assessment Criteria Notes: 1) The actual state includes: a. a list of proposed changes to the desired state; b. a list of approved changes to the actual state, likely derived from the desired state specification; and c. the date the change was proposed/approved. 2) The desired state includes: a. the time frame within which proposed items should be approved or rejected; and b. the time frame within which approved changes should be implemented in the actual state. 3) A defect occurs when a device in the assessment boundary: a. includes a proposed change that has not been addressed within the time allowed in 2(a); and/or b. includes an approved change that has not been implemented within the time frame specified in 2(b).	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L09	Reject Proposed Change	DSM
HWAM-L09	Approve Proposed Change	DSM
HWAM-L09	Accept Risk	RskEx
HWAM-L09	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L09	Low	AC-19-a	AC-19(a)
HWAM-L09	Moderate	CM-03-b	CM-3(b)
HWAM-L09	Moderate	CM-03-c	CM-3(c)
HWAM-L09	Moderate	CM-03-d	CM-3(d)
HWAM-L09	Moderate	CM-03-f	CM-3(f)
HWAM-L09	Moderate	CM-03-g	CM-3(g)
HWAM-L09	High	CM-03-z-01-a	CM-3(1)(a)
HWAM-L09	High	CM-03-z-01-b	CM-3(1)(b)
HWAM-L09	High	CM-03-z-01-c	CM-3(1)(c)

3.2.2.10 Ensure Adequate Record Retention *Sub-Capability and Defect Check HWAM-L10*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure adequate record retention	Ensure adequate historical records of HWAM ISCM data are kept in support of forensics and other risk management activities.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L10	Records retention too short	Records of actual state and/or desired state specification are not retained for the required period.	Assessment Criteria Notes: 1) The actual state includes data from actual state collection, by collection period. 2) The desired state includes: a. the required record retention period; and b. check summary data to verify the complete recording of each collection cycle, e.g., i. record counts by type; and ii. hash of complete dataset, or equivalent. 3) A defect occurs when data for a collection cycle: a. is missing in its entirety during the retention period; or b. application of the check summary indicated the collection has been altered.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L10	Restore from Backup	ISCM-OPS
HWAM-L10	Accept Risk	RskEx
HWAM-L10	Ensure Correct Response	ISCM-OPS

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L10	Moderate	CM-03-e	CM-3(e)

3.2.2.11 Ensure One-to-One Device Assignment to Authorization Boundary *Sub-Capability and Defect Check HWAM-L11*

The purpose of this sub-capability is defined as follows:

Sub-Capability Name	Sub-Capability Purpose
Ensure one-to-one device assignment to authorization boundary	Ensure device-level accountability and reduce duplication of effort by verifying that each device is in one and only one authorization boundary.

The defect check to assess whether this sub-capability is operating effectively is defined as follows:

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-L11	Device assignment to authorization boundary is not 1:1	A device in the desired state is either not listed in any authorization boundary or is listed in more than one authorization boundary.	Assessment Criteria Notes: 1) The actual state includes the data from the desired state specifications for all authorization boundaries indicating which devices are assigned to which authorization boundaries. 2) The desired state includes details specified in the component inventory regarding the authorization boundary (system) to which the device belongs. 3) A defect occurs when: a. a device is not listed in any authorization boundary; or b. a device is listed in more than one authorization boundary.	TBD

Example Responses: The following potential responses (with example assignments) are common actions and are appropriate when defects are discovered in this sub-capability. The example assignments do not change the overall management responsibilities defined in other NIST guidance. Moreover, the response actions and responsibilities can be customized by each organization to best adapt to local circumstances.

Defect Check ID	Potential Response Action	Primary Responsibility
HWAM-L11	Add to boundary if in none	DSM
HWAM-L11	Remove from all boundaries except the correct one	DSM
HWAM-L11	Accept Risk	RskEx
HWAM-L11	Ensure Correct Response	DSM

Supporting Control Items: This sub-capability is supported by the following control items. Thus, if any of the following supporting controls fail, the defect check fails and overall risk is likely to increase.

Defect Check ID	Baseline	Sortable Control Item Code	SP 800-53 Control Item Code
HWAM-L11	Moderate	CM-08-z-05-z	CM-8(5)

3.2.3 Security Impact of Each Sub-Capability on an Attack Step Model

Table 6 shows the primary ways the defect checks derived from the SP 800-53 security controls contribute to blocking attacks/event as described in Figure 1: HWAM Impact on an Attack Step Model.

Table 6: Mapping of Attack Steps to Security Sub-Capability

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Prevent unauthorized devices	Prevent or reduce the presence of unauthorized devices thus reducing the number of potentially malicious or high-risk devices.
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Reduce exploitation of devices before removal, during use elsewhere, and after return	Prevent exploitation of devices before removal, during use elsewhere, and after return (or other mobile use) by a) appropriately hardening the device prior to removal; b) checking for organizational data before removal; and c) sanitizing the device before introduction or reintroduction into the assessment boundary.
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Reduce insider threat of unauthorized device	Use separation of duties (i.e., requiring multiple persons to authorize adding a device to the authorization boundary) to limit the ability of a single careless or malicious insider to authorize high-risk devices. Note 1: The organization might choose to use access restrictions to enforce the separation of duties. If so, that would be assessed under the PRIV capability. What is assessed here is that the separation of duties occurs. Note 2: See HWAM-L11 for authorization boundary.

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Reduce denial of service attacks from missing required devices	Prevent or reduce denial of service attacks and/or attacks on resilience by ensuring that all required devices are present in the assessment boundary.
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Restrict Device Ownership	Ensure that devices not owned by the organization are not connected in the assessment boundary, or that the devices are authorized for connection only in accordance with organizationally-defined restrictions.
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Reduce unauthorized components	Detect and remove unauthorized subcomponents and/or subcomponent types to implement least functionality in order to prevent or reduce the introduction of subcomponent and subcomponent types that could enable attacks.
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Verify ongoing business need for device	Require periodic and/or event-driven consideration of whether a device is still needed for system functionality to fulfill mission requirements in support of least functionality). Note: Good practice dictates that DMs review managed devices and System Owners review devices functionally required within the authorization boundary as well as identifying non-supportable/end-of-life devices in a timely manner.

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
2) Initiate Attack Internally	The attacker is inside the boundary and initiates attack on some assessment object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gain physical access to restricted facility.	Ensure needed changes are approved or disapproved in a timely manner	Ensure that needed changes are approved or disapproved in a timely manner by flagging requested changes not considered (approved or disapproved) in a timely manner as risks.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Prevent unauthorized devices	Prevent or reduce the presence of unauthorized devices thus reducing the number of potentially malicious or high-risk devices.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Reduce number of devices without assigned device manager	Prevent or reduce the number of devices without an assigned device manager within the assessment boundary, thus reducing delay in mitigating device defects (when found).

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Reduce exploitation of devices before removal, during use elsewhere, and after return	Prevent exploitation of devices before removal, during use elsewhere, and after return (or other mobile use) by a) appropriately hardening the device prior to removal; b) checking for organizational data before removal; and c) sanitizing the device before introduction or reintroduction into the assessment boundary.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Reduce insider threat of unauthorized device	Use separation of duties (i.e., requiring multiple persons to authorize adding a device to the authorization boundary) to limit the ability of a single careless or malicious insider to authorize high-risk devices. Note 1: The organization might choose to use access restrictions to enforce the separation of duties. If so, that would be assessed under the PRIV capability. What is assessed here is that the separation of duties occurs. Note 2: See HWAM-L11 for authorization boundary.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Reduce denial of service attacks from missing required devices	Prevent or reduce denial of service attacks and/or attacks on resilience by ensuring that all required devices are present in the assessment boundary.

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Restrict Device Ownership	Ensure that devices not owned by the organization are not connected in the assessment boundary, or that the devices are authorized for connection only in accordance with organizationally-defined restrictions.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Reduce unauthorized components	Detect and remove unauthorized subcomponents and/or subcomponent types to implement least functionality in order to prevent or reduce the introduction of subcomponent and subcomponent types that could enable attacks.
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Verify ongoing business need for device	Require periodic and/or event driven consideration of whether a device is still needed for system functionality to fulfill mission requirements in support of least functionality). Note: Good practice dictates that DMs review managed devices and System Owners review devices functionally required within the authorization boundary as well as identifying non-supportable/end-of-life devices in a timely manner.

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
3) Gain Foothold	The attacker has gained entry to the assessment object and achieves enough actual compromise to gain a foothold, but without persistence. Examples include: Unauthorized user successfully logs in with authorized credentials; browser exploit code successfully executed in memory and initiates call back; person gains unauthorized access to server room.	Ensure needed changes are approved or disapproved in a timely manner	Ensure that needed changes are approved or disapproved in a timely manner by flagging requested changes not considered (approved or disapproved) in a timely manner as risks.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Prevent unauthorized devices	Prevent or reduce the presence of unauthorized devices thus reducing the number of potentially malicious or high-risk devices.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Reduce exploitation of devices before removal, during use elsewhere, and after return	Prevent or reduce exploitation of devices before removal, during use elsewhere, and after return (or other mobile use) by a) appropriately hardening the device prior to removal; b) checking for organizational data before removal; and c) sanitizing the device before introduction or reintroduction into the assessment boundary.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Reduce insider threat of unauthorized device	Use separation of duties (i.e., requiring multiple persons to authorize adding a device to the authorization boundary) to limit the ability of a single careless or malicious insider to authorize high-risk devices. Note 1: The organization might choose to use access restrictions to enforce the separation of duties. If so, that would be assessed under the PRIV capability. What is assessed here is that the separation of duties occurs. Note 2: See HWAM-L11 for authorization boundary.

Attack Step	Attack Step Description	Sub-Capability Name	Sub-Capability Purpose
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Restrict Device Ownership	Ensure that devices not owned by the organization are not connected in the assessment boundary, or that the devices are authorized for connection only in accordance with organizationally-defined restrictions.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Reduce unauthorized components	Detect and remove unauthorized subcomponents and/or subcomponent types to implement least functionality in order to prevent or reduce the introduction of subcomponent and subcomponent types that could enable attacks.
6) Achieve Attack Objective	The attacker achieves an objective. Loss of confidentiality, integrity, or availability of data or system capability. Examples include: Exfiltration of files; modification of database entries; deletion of file or application; denial of service; disclosure of PII.	Verify ongoing business need for device	Require periodic and/or event driven consideration of whether a device is still needed for system functionality to fulfill mission requirements in support of least functionality. Note: Good practice dictates that DMs review managed devices and System Owners review devices functionally required within the authorization boundary as well as identifying non-supportable/end-of-life devices in a timely manner.

3.3 HWAM Control (Item) Security Assessment Plan Narrative Tables and Templates

The security assessment plan narratives in this section are designed to provide the core of an assessment plan for the automated assessment, as described in Section 6 of Volume 1 of this NISTIR. The narratives are supplemented by the other material in this section, including defect check tables (defining the tests to be used) and are summarized in the Control Allocation Tables in Section 3.4.

The roles referenced in the narratives match the roles defined by NIST in relevant special publications (SP 800-37, etc.) and/or the HWAM-specific roles defined in Section 2.7. The roles can be adapted and/or customized to the organization as described in the introduction to Section 3.

The determination statements listed here have been derived from the relevant control item language, specifically modified by the following adjustments:

(1) The phrase {for devices and device components} has been added where necessary for control items that apply to more areas than just HWAM. This language tailors the control item to remain within HWAM. In this case, the same control item is likely to appear in other capabilities with the relevant scoping for that capability. For example, most Configuration Management (CM) family controls apply not only to hardware CM, but also to software CM. Only the hardware CM aspect is relevant to the HWAM capability, so that is what is covered in this volume.

(2) The phrases {actual state} or {desired state specification} have been added to determination statements where both actual and desired state are needed for automated testing but where this was implicit in the original statement of the control. For example, CM-8a has two determination statements that are identical except that determination statement CM-8a(1) applies to the actual state, and determination statement CM-8a(2) applies to the desired state specification.

(3) Where a control item includes inherently different actions that are best assessed by different defect checks (typically, because the assessment criteria are different), the control item may be divided into multiple HWAM-applicable determination statements.

(4) Part of a control item may not apply to HWAM, while another part does. For example, consider the control item CM-8(3b). To address this issue, the determination statements in this volume include only the portion of the control item applicable to the HWAM capability. The portion of the control item that does not apply is documented by a note under the control item and included with other capabilities, as appropriate.

3.3.1 Outline Followed for Each Control Item

The literal text of the control item follows the heading *Control Item Text*.

There may be one or more determination statements for each control item. Each determination statement is documented in a table, noting the:

- determination statement ID;
- determination statement text;
- implemented by (responsibility);
- assessment boundary;
- assessment responsibility;
- assessment method;
- selected column (TBD by the organization);
- rationale for risk acceptance (thresholds) (TBD by the organization);
- frequency of assessment;[5] and
- impact of not implementing the defect check (TBD by the organization).

This is followed by a table showing the defect checks (and related sub-capability) that might be caused to fail if this control fails.

This text provides a template for the organization to edit, as described in Section 3.1.

3.3.2 Outline Organized by Baselines

This section includes security control items selected in the SP 800-53 Low, Moderate, and High baselines and that support the HWAM capability. For convenience, the control items are presented in three sections as follows:

(1) **Low Baseline Control Items** (Section 3.3.3). Security control items in the low baseline, which are required for all systems.

(2) **Moderate Baseline Control Items** (Section 3.3.4). Security control items in the moderate baseline, which are also required for the high baseline.

(3) **High Baseline Control Items** (Section 3.3.5). Security control items that are required only for the high baseline.

Table 7 illustrates the applicability of the security control items to each baseline.

[5] While automated tools may be able to assess as frequently as every 3-4 days, organizations determine the appropriate assessment frequency in accordance with the ISCM strategy.

Table 7: Applicability of Control Items

FIPS-199[a] (SP 800-60)[b] System Impact Level	**(1) Low Control Items (Section 3.3.3)**	**(2) Moderate Control Items (Section 3.3.4)**	**(3) High Control Items (Section 3.3.5)**
Low	Applicable	▨	▨
Moderate	Applicable	Applicable	▨
High	Applicable	Applicable	Applicable

[a] FIPS-199 defines Low, Moderate, and High overall potential impact designations.
[b] See SP 800-60, Section 3.2.

3.3.3 Low Baseline Security Control Item Narratives

3.3.3.1 Control Item AC-19: ACCESS CONTROL FOR MOBILE DEVICES

Control Item Text:

Control: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

Note: Parts of the control item are assigned to other capabilities, as follows: BEHAVE: usage restrictions; BOUND-N: connection requirements; SE implementation guidance.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
AC-19(a)(1)	Determine if the organization: Establishes configuration requirements for organization-controlled mobile devices (and subcomponents).

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency Of Assessment	Impact of not implementing
AC-19(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	**Defect Check ID**	**Defect Check Name**	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices being established or implemented related to this control item*** might be the cause of ...
AC-19(a)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
AC-19(a)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
AC-19(a)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.3.2 Control Item AC-19(b): ACCESS CONTROL FOR MOBILE DEVICES

Control Item Text:

Control: The organization:

b. Authorizes the connection of mobile devices to organizational systems.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
AC-19(b)(1)	Determine if the organization: authorizes the connection of mobile devices to organizational system {considering any subcomponents}

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
AC-19(b)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	Rationale If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the authorization of the connection of mobile devices to organizational systems related to this control item*** might be the cause of ...
AC-19(b)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
AC-19(b)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.

3.3.3.3 Control Item CM-8(a): SYSTEM COMPONENT INVENTORY

Control Item Text:

Control: The organization:

a. Develops and documents an inventory of system components that:

1. Accurately reflects the current system;
2. Includes all components within the authorization boundary of the system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [Assignment: organization-defined information deemed necessary to achieve effective system component accountability].

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(a)(1)	Determine if the organization: a. Develops and documents an inventory of system components {for devices and device components} that: 1. Accurately reflects the current system; 2. Includes all components within the authorization boundary of the system;

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in an inventory of the {devices and device subcomponents of the} system that includes all components within the authorization boundary being developed/documented or being accurate related to this control item*** might be the cause of ...
CM-8(a)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-8(a)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-8(a)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-8(a)(1)	HWAM-L08	Missing required device data	a device missing required data being found in the assessment boundary.
CM-8(a)(1)	HWAM-Q01	Non-reporting devices	a device failing to report within the specified time frame.
CM-8(a)(1)	HWAM-Q03	Low completeness metric	completeness of overall ISCM reporting not meeting the threshold.
CM-8(a)(1)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-8(a)(2)	Determine if the organization: a. Develops and documents an inventory of system components {for devices and device components} that: 3. Is at the level of granularity deemed necessary for tracking and reporting;

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(a)(2)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "accurately" including "all {desired state} components within the authorization boundary of the system" in this control item*** might be the cause of . . .
CM-8(a)(2)	HWAM-F01	Unauthorized Devices	the presence of unauthorized devices.
CM-8(a)(2)	HWAM-L03	Required Device not Installed	lack of a required device in the assessment boundary.
CM-8(a)(2)	HWAM-L06	Subcomponents not Authorized	a device with unauthorized subcomponents in the assessment boundary.
CM-8(a)(2)	HWAM-L08	Required Device Data	a device with missing required data.

Determination Statement 3:

Determination Statement ID	Determination Statement Text
CM-8(a)(3)	Determine if the organization: a. Develops and documents an inventory of system components {for devices and device components} that: 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective system component accountability];

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(a)(3)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the inventory of system components {devices and device subcomponents} reflecting the organization-defined information deemed necessary to achieve effective system component accountability related to this control item*** might be the cause of ...
CM-8(a)(3)	HWAM-L08	Missing required device data	a device missing required data being found in the assessment boundary.

3.3.3.4 Control Item CM-8(b): SYSTEM COMPONENT INVENTORY

Control Item Text:

Control: The organization:

b. Reviews and updates the system component inventory [Assignment: organization-defined frequency].

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(b)(1)	Determine if the organization: b. Reviews and updates the system component inventory {for devices and device components} [Assignment: organization-defined frequency].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in conducting reviews and updates of the {actual state} system component inventory {for devices and device components}" with the "organization-defined frequency" related to this control item*** might be the cause of ...
CM-8(b)(1)	HWAM-Q04	Low Timeliness Metric	low timeliness of overall ISCM reporting.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-8(b)(2)	Determine if the organization: b. Reviews and updates the system component inventory {for devices and device components} [Assignment: organization-defined frequency].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(b)(2)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the system component {devices and device subcomponents} inventory being reviewed and updated with the organization-defined frequency" related to this control item*** might be the cause of ...
CM-8(b)(2)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-8(b)(2)	HWAM-L08	Missing required device data	a device missing required data being found in the assessment boundary.

3.3.3.5 Control Item CM-8(4): SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

Control Item Text:

> The organization includes in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(4)(1)	Determine if the organization: Includes in the system {hardware} component {desired state} inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(4)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the name, position, or role of the individuals responsible/accountable for administering those components {devices and device subcomponents} being included in the system component inventory related to this control item*** might be the cause of ...
CM-8(4)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.

3.3.3.6 Control Item PS-4(d): PERSONNEL TERMINATION

Control Item Text:

Control: The organization, upon termination of individual employment:

d. Retrieves all security-related organizational system-related property which is {a device or subcomponent}.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
PS-4(d)(1)	Determine if the organization: upon termination of individual employment: d. Retrieves all security-related organizational system-related property {devices and subcomponents};

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
PS-4(d)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	Rationale If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in assigned security-related devices and subcomponents being retrieved on employee termination related to this control item*** might be the cause of ...
PS-4(d)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
PS-4(d)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.

3.3.3.7 Control Item SC-15(a): COLLABORATIVE COMPUTING DEVICES

Control Item Text:

Control: The system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and

Determination Statement 1:

Determination Statement ID	Determination Statement Text
SC-15(a)(1)	Determine if the organization: prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
SC-15(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	Rationale If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the process to authorize collaborative computing devices in this control item*** might be the cause of ...
SC-15(a)(1)	HWAM-F01	Unauthorized Devices	the presence of unauthorized devices.
SC-15(a)(1)	HWAM-L01	Devices Moving into/out of the Assessment Boundary	devices not adequately prepared for movement into or out of the assessment boundary.

3.3.3.8 Control Item SC-15(b): COLLABORATIVE COMPUTING DEVICES

Control Item Text:

Control: The system:

b. Provides an explicit indication of use to users physically present at the device.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
SC-15(b)(1)	Determine if the organization: provides an explicit indication of use {of collaborative computing} to users physically present at the devices

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
SC-15(b)(1)	MAN	ISCM-TN	ISCM-Sys	TBD				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

N/A because tested manually.

3.3.4 Moderate Baseline Security Control Item Narratives

3.3.4.1 Control Item AC-19(5): ACCESS CONTROL FOR MOBILE DEVICES | PERSONALLY OWNED DEVICES

Control Item Text:

The organization [Selection: restricts; prohibits] the connection of personally-owned, mobile devices to organizational systems.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
AC-19(5)(1)	Determine if the organization: [Selection: restricts; prohibits] the connection of personally-owned, mobile devices to organizational systems.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
AC-19(5)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the connection of personally owned mobile devices to organizational systems being restricted or prohibited related to this control item*** might be the cause of ...
AC-19(5)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
AC-19(5)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.

3.3.4.2 Control Item AC-20(2): USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES

Control Item Text:

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external systems.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
AC-20(2)(1)	Determine if the organization: [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external systems

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
AC-20(2)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the use of removable storage devices being restricted or prohibited related to this control item*** might be the cause of ...
AC-20(2)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
AC-20(2)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
AC-20(2)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.

3.3.4.3 Control Item CM-2(7)(a): BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Control Item Text:

The organization:

(a) Issues [Assignment: organization-defined systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-2(7)(a)(1)	Determine if the organization: issues [Assignment: organization-defined … devices {and subcomponents} with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-2(7)(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in devices or device subcomponents of systems that are securely configured in accordance with organization-defined configurations are issued to individuals traveling to locations that the organization deems to be of significant risk related to this control item*** might be the cause of ...
CM-2(7)(a)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.

3.3.4.4 Control Item CM-2(7)(b): BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Control Item Text:

The organization:

(b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-2(7)(b)(1)	Determine if the organization: Applies [Assignment: organization-defined security safeguards] to the devices {and device subcomponents} when the individuals return.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-2(7)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "organization-defined security safeguards" being applied to the {devices and device subcomponents of the} systems when " individuals return" from "locations that the organization deems to be of significant risk" related to this control item*** might be the cause of ...
CM-2(7)(b)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.

3.3.4.5 Control Item CM-3(a): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

a. Determines the types of changes to the system that are configuration-controlled.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(a)(1)	Determine if the organization: a. Determines the types of changes to the {devices and device subcomponents of the} system that are configuration-controlled.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(a)(1)	DSM	TBD	MAN	TBD				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

N/A because tested manually.

3.3.4.6 Control Item CM-3(b): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

b. Reviews proposed configuration-controlled changes to the system and approves or disapproves such changes with explicit consideration for security impact analyses;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(b)(1)	Determine if the organization: b. Reviews proposed configuration-controlled changes to the {devices and device subcomponents of the} system and approves or disapproves such changes.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(b)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "proposed configuration-controlled changes to the" devices or device subcomponents being reviewed and approved/disapproved related to this control item*** might be the cause of ...
CM-3(b)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(b)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(b)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(b)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(b)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(b)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(b)(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.
CM-3(b)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(b)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(b)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-3(b)(2)	Determine if the organization: b. explicitly considers security impact analysis when reviewing proposed configuration-controlled changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(b)(2)	MAN	TBD	MAN	TBD				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

N/A because assessed manually.

3.3.4.7 Control Item CM-3(c): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

c. Documents configuration change decisions associated with the system;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(c)(1)	Determine if the organization: c. Documents configuration change decisions associated with the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(c)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "configuration change decisions associated with the {devices and device subcomponents of the} system" being documented and entered into the desired state specification related to this control item*** might be the cause of ...
CM-3(c)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(c)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(c)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(c)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(c)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(c)(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.
CM-3(c)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(c)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(c)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.4.8 Control Item CM-3(d): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

d. Implements approved configuration-controlled changes to the system;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(d)(1)	Determine if the organization: d. Implements approved configuration-controlled changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(d)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "approved configuration-controlled changes to the" devices or device subcomponents of the system" being implemented related to this control item*** might be the cause of ...
CM-3(d)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(d)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(d)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(d)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(d)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(d)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(d)(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.
CM-3(d)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(d)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(d)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.4.9 Control Item CM-3(e): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

e. Retains records of configuration-controlled changes to the system for [Assignment: organization-defined time period];

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(e)(1)	Determine if the organization: e. Retains records of configuration-controlled changes to the {devices and device subcomponents of the} system for [Assignment: organization-defined time period].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(e)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in "records of configuration-controlled changes to the {devices and device subcomponents of the} system" being retained for the required time period related to this control item*** might be the cause of ...
CM-3(e)(1)	HWAM-L10	Records retention too short	records of the actual/desired state not being retained for the required period.

3.3.4.10 Control Item CM-3(f): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

f. Audits and reviews activities associated with configuration-controlled changes to the system

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(f)(1)	Determine if the organization: f. Audits activities associated with configuration-controlled changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(f)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in activities associated with configuration-controlled changes to the {devices and device subcomponents of the} system being audited related to this control item*** might be the cause of ...
CM-3(f)(1)	HWAM-Q01	Non-reporting devices	a device failing to report within the specified time frame.
CM-3(f)(1)	HWAM-Q02	Non-reporting defect checks	specific defect checks failing to report.
CM-3(f)(1)	HWAM-Q03	Low completeness metric	completeness of overall ISCM reporting not meeting the threshold.
CM-3(f)(1)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-3(f)(2)	Determine if the organization: f. Reviews activities associated with configuration-controlled changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(f)(2)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in activities associated with configuration-controlled changes to the {devices and device subcomponents of the} system being reviewed related to this control item*** might be the cause of ...
CM-3(f)(2)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(f)(2)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.
CM-3(f)(2)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

3.3.4.11 Control Item CM-3(g): CONFIGURATION CHANGE CONTROL

Control Item Text:

Control: The organization:

g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions].

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(g)(1)	Determine if the organization: g. Coordinates configuration change control activities {of devices and device subcomponents} through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(g)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	Rationale If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in coordination of configuration change control activities related to {devices and device subcomponents of the} of the system being provided via an established configuration change control element related to this control item*** might be the cause of ...
CM-3(g)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(g)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(g)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(g)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(g)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(g)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(g)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(g)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(g)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-3(g)(2)	Determine if the organization: g. Provides oversight for configuration change control activities {of devices and device subcomponents} through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(g)(2)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in oversight of configuration change control activities related to {devices and device subcomponents of the} of the system being provided via an established configuration change control element related to this control item*** might be the cause of ...
CM-3(g)(2)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(g)(2)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.
CM-3(g)(2)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

3.3.4.12 Control Item CM-3(2): CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES

Control Item Text:

The organization tests, validates, and documents changes to the system before implementing the changes on the operational system.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(2)(1)	Determine if the organization: tests, validates, and documents changes to the {devices and device subcomponents of the} system before implementing the changes on the operational system. This control should be assessed via manual reauthorization prior to placing policy in the desired state. Because it occurs as part of system engineering, it is outside the scope of this operational capability.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(2)(1)	TBD	TBD	MAN	TBD				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

N/A because assessed manually.

3.3.4.13 Control Item CM-8(1): SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

Control Item Text:

The organization updates the inventory of system components as an integral part of component installations, removals, and system updates.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(1)(1)	Determine if the organization: (1) The organization updates the inventory of system {devices and device subcomponents} as an integral part of component installations, removals, and system updates.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(1)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in updating the inventory of system {device and device subcomponents} as an integral part of component installations, removals, and system updates related to this control item*** might be the cause of ...
CM-8(1)(1)	HWAM-Q01	Non-reporting devices	a device failing to report within the specified time frame.
CM-8(1)(1)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

Determination Statement 2:

Determination Statement ID	Determination Statement Text
CM-8(1)(2)	Determine if the organization: (1) The organization updates the {desired state} inventory of {devices and device subcomponents of the} system components as an integral part of component installations, removals, and system updates.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(1)(2)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in updates to the system component {devices and device subcomponents} inventory being an integral part of component installations, removals, and system updates related to this control item*** might be the cause of ...
CM-8(1)(2)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-8(1)(2)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.

3.3.4.14 Control Item CM-8(3)(a): SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Control Item Text:

The organization:

(a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the system;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(3)(a)(1)	Determine if the organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized {devices and device subcomponents} within the system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(3)(a)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to detect the presence of unauthorized system components {devices and device subcomponents} at the organization-defined frequency being implemented related to this control item*** might be the cause of ...
CM-8(3)(a)(1)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

3.3.4.15 Control Item CM-8(3)(b): SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Control Item Text:

The organization:

(b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles].

Note: Parts of the control item are assigned to other capabilities, as follows: BEHAVE: notifies [Assignment: organization-defined personnel or roles].

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(3)(b)(1)	Determine if the organization: (b) Takes the following actions when unauthorized {devices and device subcomponents} are detected: [Selection (one or more): disables network access by such components; isolates the components].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(3)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	**Defect Check ID**	**Defect Check Name**	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in selected actions being taken by defined personnel or roles when unauthorized components {devices and device subcomponents} are detected (i.e., actual state components not found in the device inventory) related to this control item*** might be the cause of ...
CM-8(3)(b)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-8(3)(b)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.

3.3.4.16 Control Item CM-8(5): SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

Control Item Text:

The organization verifies that all components within the authorization boundary of the system are not duplicated in other system component inventories.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(5)(1)	Determine if the organization: verifies that all {devices} within the authorization boundary of the system are not duplicated in other system inventories.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(5)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the verification that components {devices and device subcomponents} within the authorization boundary of the system are duplicated in other system component inventories related to this control item*** might be the cause of ...
CM-8(5)(1)	HWAM-L11	Device assignment to authorization boundary is not 1:1.	device not being assigned correctly to one and only one authorization boundary.

3.3.4.17 Control Item MA-3(1): MAINTENANCE TOOLS | INSPECT TOOLS

Control Item Text:

> The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
MA-3(1)(1)	Determine if the organization: inspects the maintenance tools {devices and subcomponents} carried into a facility by maintenance personnel for improper or unauthorized modifications.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
MA-3(1)(1)	DM	ISCM-TN	ISCM-Sys	Test				

Note: May not find all instances, depending on frequency and completeness of assessment.

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in maintenance tools {devices and device subcomponents} brought to a facility by maintenance personnel being inspected to check for improper or unauthorized modifications related to this control item*** might be the cause of ...
MA-3(1)(1)	HWAM-F01[6]	Unauthorized devices	the presence of unauthorized devices.
MA-3(1)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
MA-3(1)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.

[6] Inspection of maintenance tools (devices) is required prior to authorizing use of such tools.

3.3.4.18 Control Item MP-7(1): MEDIA USE | PROHIBIT USE WITHOUT OWNER

Control Item Text:

The organization prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
MP-7(1)(1)	Determine if the organization: prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
MP-7(1)(1)	DM	ISCM-TN	ISCM-Sys	Test				

Note: May not find all instances, depending on frequency and completeness of assessment.

A defect in control item effectiveness will create a defect in one or more defect checks as follows:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in the use of portable storage devices with no owner not being prohibited in {the actual state of} organizational system (i.e., no policy or process exists, or the policies/processes are being followed). related to this control item*** might be the cause of ...
MP-7(1)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).

3.3.5 High Baseline Security Control Item Narratives

3.3.5.1 Control Item CM-3(1)(a): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(a) Document proposed changes to the system;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(a)(1)	Determine if the organization: employs automated mechanisms to: (a) Document proposed changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to document proposed changes to the {devices and device subcomponents of the} system being implemented related to this control item*** might be the cause of ...
CM-3(1)(a)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(1)(a)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(1)(a)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(1)(a)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(1)(a)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(1)(a)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(1)(a)(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.
CM-3(1)(a)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(1)(a)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(1)(a)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.5.2 Control Item CM-3(1)(b): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the system and request change approval;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(b)(1)	Determine if the organization: employs automated mechanisms to: (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the {devices and device subcomponents of the} system and request change approval.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(b)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to notify appropriate personnel of proposed changes to the {devices and device subcomponents of the} system and request change approval being implemented related to this control item*** might be the cause of ...
CM-3(1)(b)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(1)(b)(1)	HWAM-F02	Authorized devices without a device manager	a device manager not being assigned.
CM-3(1)(b)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
CM-3(1)(b)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(1)(b)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.
CM-3(1)(b)(1)	HWAM-L04	Restrictions on device ownership	a device not owned by the organization or by an approved owner being found in the assessment boundary (or violating other requirements for BYOD).
CM-3(1)(b)(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.
CM-3(1)(b)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.
CM-3(1)(b)(1)	HWAM-L07	Business need and/or device manager not recently verified	a device with an expired sunset date (or other trigger to review need and management) being found in the assessment boundary.
CM-3(1)(b)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.5.3 Control Item CM-3(1)(c): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(c) Highlight proposed changes to the system that have not been approved or disapproved by [Assignment: organization-defined time period];

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(c)(1)	Determine if the organization: employs automated mechanisms to: (c) Highlight proposed changes to the {devices and device subcomponents of the} system that have not been approved or disapproved by [Assignment: organization-defined time period].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(c)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to highlight proposed changes to the {devices and device subcomponents of the} system not being approved or disapproved within the established time period and thus being implemented related to this control item*** might be the cause of ...
CM-3(1)(c)(1)	HWAM-L09	Proposed changes are too old	requested changes not being addressed in a timely manner.

3.3.5.4 Control Item CM-3(1)(d): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(d) Prohibit changes to the system until designated approvals are received;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(d)(1)	Determine if the organization: employs automated mechanisms to: (d) Prohibit changes to the {devices and device subcomponents of the} system until designated approvals are received.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(d)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to prohibit changes to the {devices and device subcomponents of the} system until approval is received being implemented related to this control item*** might be the cause of ...
CM-3(1)(d)(1)	HWAM-F01	Unauthorized devices	the presence of unauthorized devices.
CM-3(1)(d)(1)	HWAM-L02	Required authorization missing	changes to system hardware not being authorized by multiple persons as required.
CM-3(1)(b)(1)	HWAM-L06	Subcomponents not authorized	a device with unauthorized subcomponents or a device lacking required subcomponents being found in the assessment boundary.

3.3.5.5 Control Item CM-3(1)(e): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(e) Document all changes to the system;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(e)(1)	Determine if the organization: employs automated mechanisms to: (e) Document all changes to the {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(e)(1)	ISCM-Sys	TBD	MAN	TBD				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

N/A because assessed manually.

3.3.5.6 Control Item CM-3(1)(f): CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Control Item Text:

The organization employs automated mechanisms to:

(f) Notify [Assignment: organization-defined personnel] when approved changes to the system are completed.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-3(1)(f)(1)	Determine if the organization: employs automated mechanisms to: (f) Notify [Assignment: organization-defined personnel] when approved changes to the {devices and device subcomponents of the} system are completed.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-3(1)(f)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to notify designated personnel when approved changes to the {devices and device subcomponents of the} system are being implemented related to this control item*** might be the cause of ...
CM-3(1)(f)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.

3.3.5.7 Control Item CM-8(2): SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

Control Item Text:

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of system components.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
CM-8(2)(1)	Determine if the organization: employs automated mechanisms to: help maintain an up-to-date, complete, accurate, and readily available {actual state} inventory of {devices and device subcomponents of the} system.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
CM-8(2)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in automated mechanisms to help maintain and up-to-date, complete, accurate, and readily available system component {devices and device subcomponents} inventory being implemented related to this control item*** might be the cause of ...
CM-8(2)(1)	HWAM-Q01	Non-reporting devices	a device failing to report within the specified time frame.
CM-8(2)(1)	HWAM-Q03	Low completeness metric	completeness of overall ISCM reporting not meeting the threshold.
CM-8(2)(1)	HWAM-Q04	Poor timeliness metric	poor timeliness of overall ISCM reporting.

3.3.5.8 Control Item MA-3(3)(a): MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

Control Item Text:

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
MA-3(3)(a)(1)	Determine if the organization: prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment [before removal].

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
MA-3(3)(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in verification that organizational information being contained on maintenance equipment {devices and device subcomponents} to be removed related to this control item*** might be the cause of ...
MA-3(3)(a)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
MA-3(3)(a)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.

3.3.5.9 Control Item MA-3(3)(b): MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

Control Item Text:

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(b) Sanitizing or destroying the equipment;

Determination Statement 1:

Determination Statement ID	Determination Statement Text
MA-3(3)(b)(1)	Determine if the organization: prevents the unauthorized removal of maintenance equipment containing organizational information by: (b) Sanitizing or destroying the equipment.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
MA-3(3)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in maintenance equipment {devices and device subcomponents} being sanitized or destroyed before removal related to this control item*** might be the cause of ...
MA-3(3)(b)(1)	HWAM-L01	Devices moving into/out of the assessment boundary	devices not being adequately prepared for movement into or out of the assessment boundary.
MA-3(3)(b)(1)	HWAM-L03	Required device not installed	a required device not being found in the assessment boundary.

Note: May not find all instances, depending on the frequency and completeness of assessment.

3.3.5.10 Control Item SA-12: SUPPLY CHAIN PROTECTION

Control Item Text:

> Control: The organization protects against supply chain threats to the system, system component, or system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

Determination Statement 1:

Determination Statement ID	Determination Statement Text
SA-12(1)	Determine if the organization: protects against supply chain threats to the system {devices and device subcomponents } by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
SA-12(1)	DSM	ISCM-TN	ISCM-Sys	Test				

A failure in control item effectiveness results in a defect in one or more of the following defect checks:

Determination Statement ID	Defect Check ID	Defect Check Name	**Rationale** If an [organization-defined measure] for this defect check is above [the organization-defined threshold], ***then defects in organization-defined security safeguards/mechanisms being employed to protect against supply-chain threats to the {devices and device subcomponents of the} system related to this control item*** might be the cause of ...
SA-12(1)	HWAM-L05	Unapproved supplier and/or manufacturer	a device with an unapproved supplier and/or manufacturer being found in the assessment boundary.

3.4 Control Allocation Tables (CATs)

Table 8: Low Baseline Control (Item) Allocation Table, Table 9: Moderate Baseline Control (Item) Allocation Table, and Table 10: High Baseline Control (Item) Allocation Table provide the low, moderate, and high baseline control allocation tables, respectively. This is a summary of the material in the security plan assessment narrative for each determination statement in Section 3.3. It provides a concise summary of the assessment plan.

3.4.1 Low Baseline Control Allocation Table

Table 8: Low Baseline Control (Item) Allocation Table

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
AC-19(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
AC-19(b)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(a)(2)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(a)(3)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-8(b)(2)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(4)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
PS-4(d)(1)	DM	ISCM-TN	ISCM-Sys	Test				
SC-15(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				
SC-15(b)(1)	MAN	ISCM-TN	ISCM-Sys	TBD				

3.4.2 Moderate Baseline Control Allocation Table

Table 9: Moderate Baseline Control (Item) Allocation Table

Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
AC-19(5)(1)	DM	ISCM-TN	ISCM-Sys	Test				
AC-20(2)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-2(7)(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-2(7)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-3(a)(1)	DSM	TBD	MAN	TBD				
CM-3(b)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-3(b)(2)	MAN	ISCM-TN	MAN	TBD				
CM-3(c)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-3(d)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-3(e)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-3(f)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-3(f)(2)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-3(g)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-3(g)(2)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-3(2)(1)	TBD	TBD	MAN	TBD				
CM-8(1)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(1)(2)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(3)(a)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(3)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-8(5)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
MA-3(1)(1)	DM	ISCM-TN	ISCM-Sys	Test				
MP-7(1)(1)	DM	ISCM-TN	ISCM-Sys	Test				

3.4.3 High Baseline Control Allocation Table

Table 10: High Baseline Control (Item) Allocation Table

Impact Level	Determination Statement ID	Implemented By	Assessment Boundary	Assessment Responsibility	Assessment Methods	Selected	Rationale for Risk Acceptance	Frequency of Assessment	Impact of not implementing
3	CM-3(1)(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
3	CM-3(1)(b)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
3	CM-3(1)(c)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
3	CM-3(1)(d)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
3	CM-3(1)(e)(1)	ISCM-Sys	TBD	MAN	TBD				
3	CM-3(1)(f)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
3	CM-8(2)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
3	MA-3(3)(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				
3	MA-3(3)(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				
3	SA-12(1)	DSM	ISCM-TN	ISCM-Sys	Test				

Appendix A. Traceability of HWAM Control Items to Example Attack Steps

Example Attack Step	Sortable Control Item Code	SP 800-53 Control Item Code
2) Initiate Attack Internally	AC-19-a	AC-19(a)
2) Initiate Attack Internally	AC-19-b	AC-19(b)
2) Initiate Attack Internally	AC-19-z-05-z	AC-19(5)
2) Initiate Attack Internally	AC-20-z-02-z	AC-20(2)
2) Initiate Attack Internally	CM-02-z-07-a	CM-2(7)(a)
2) Initiate Attack Internally	CM-02-z-07-b	CM-2(7)(b)
2) Initiate Attack Internally	CM-03-b	CM-3(b)
2) Initiate Attack Internally	CM-03-c	CM-3(c)
2) Initiate Attack Internally	CM-03-d	CM-3(d)
2) Initiate Attack Internally	CM-03-f	CM-3(f)
2) Initiate Attack Internally	CM-03-g	CM-3(g)
2) Initiate Attack Internally	CM-03-z-01-a	CM-3(1)(a)
2) Initiate Attack Internally	CM-03-z-01-b	CM-3(1)(b)
2) Initiate Attack Internally	CM-03-z-01-c	CM-3(1)(c)
2) Initiate Attack Internally	CM-03-z-01-d	CM-3(1)(d)
2) Initiate Attack Internally	CM-03-z-01-f	CM-3(1)(f)
2) Initiate Attack Internally	CM-08-a	CM-8(a)
2) Initiate Attack Internally	CM-08-b	CM-8(b)
2) Initiate Attack Internally	CM-08-z-01-z	CM-8(1)
2) Initiate Attack Internally	CM-08-z-03-b	CM-8(3)(b)
2) Initiate Attack Internally	MA-03-z-01-z	MA-3(1)
2) Initiate Attack Internally	MA-03-z-03-a	MA-3(3)(a)
2) Initiate Attack Internally	MA-03-z-03-b	MA-3(3)(b)
2) Initiate Attack Internally	MP-07-z-01-z	MP-7(1)
2) Initiate Attack Internally	PS-04-d	PS-4(d)
2) Initiate Attack Internally	SC-15-a	SC-15(a)
3) Gain Foothold	AC-19-a	AC-19(a)
3) Gain Foothold	AC-19-b	AC-19(b)
3) Gain Foothold	AC-19-z-05-z	AC-19(5)
3) Gain Foothold	AC-20-z-02-z	AC-20(2)
3) Gain Foothold	CM-02-z-07-a	CM-2(7)(a)
3) Gain Foothold	CM-02-z-07-b	CM-2(7)(b)
3) Gain Foothold	CM-03-b	CM-3(b)

Example Attack Step	Sortable Control Item Code	SP 800-53 Control Item Code
3) Gain Foothold	CM-03-c	CM-3(c)
3) Gain Foothold	CM-03-d	CM-3(d)
3) Gain Foothold	CM-03-f	CM-3(f)
3) Gain Foothold	CM-03-g	CM-3(g)
3) Gain Foothold	CM-03-z-01-a	CM-3(1)(a)
3) Gain Foothold	CM-03-z-01-b	CM-3(1)(b)
3) Gain Foothold	CM-03-z-01-c	CM-3(1)(c)
3) Gain Foothold	CM-03-z-01-d	CM-3(1)(d)
3) Gain Foothold	CM-03-z-01-f	CM-3(1)(f)
3) Gain Foothold	CM-08-a	CM-8(a)
3) Gain Foothold	CM-08-b	CM-8(b)
3) Gain Foothold	CM-08-z-01-z	CM-8(1)
3) Gain Foothold	CM-08-z-03-b	CM-8(3)(b)
3) Gain Foothold	CM-08-z-04-z	CM-8(4)
3) Gain Foothold	MA-03-z-01-z	MA-3(1)
3) Gain Foothold	MA-03-z-03-a	MA-3(3)(a)
3) Gain Foothold	MA-03-z-03-b	MA-3(3)(b)
3) Gain Foothold	MP-07-z-01-z	MP-7(1)
3) Gain Foothold	PS-04-d	PS-4(d)
3) Gain Foothold	SC-15-a	SC-15(a)
6) Achieve Attack Objective	AC-19-a	AC-19(a)
6) Achieve Attack Objective	AC-19-b	AC-19(b)
6) Achieve Attack Objective	AC-19-z-05-z	AC-19(5)
6) Achieve Attack Objective	AC-20-z-02-z	AC-20(2)
6) Achieve Attack Objective	CM-02-z-07-a	CM-2(7)(a)
6) Achieve Attack Objective	CM-02-z-07-b	CM-2(7)(b)
6) Achieve Attack Objective	CM-03-b	CM-3(b)
6) Achieve Attack Objective	CM-03-c	CM-3(c)
6) Achieve Attack Objective	CM-03-d	CM-3(d)
6) Achieve Attack Objective	CM-03-f	CM-3(f)
6) Achieve Attack Objective	CM-03-g	CM-3(g)
6) Achieve Attack Objective	CM-03-z-01-a	CM-3(1)(a)
6) Achieve Attack Objective	CM-03-z-01-b	CM-3(1)(b)
6) Achieve Attack Objective	CM-03-z-01-d	CM-3(1)(d)
6) Achieve Attack Objective	CM-08-a	CM-8(a)
6) Achieve Attack Objective	CM-08-b	CM-8(b)
6) Achieve Attack Objective	CM-08-z-01-z	CM-8(1)
6) Achieve Attack Objective	CM-08-z-03-b	CM-8(3)(b)

Example Attack Step	Sortable Control Item Code	SP 800-53 Control Item Code
6) Achieve Attack Objective	MA-03-z-01-z	MA-3(1)
6) Achieve Attack Objective	MA-03-z-03-a	MA-3(3)(a)
6) Achieve Attack Objective	MA-03-z-03-b	MA-3(3)(b)
6) Achieve Attack Objective	MP-07-z-01-z	MP-7(1)
6) Achieve Attack Objective	PS-04-d	PS-4(d)
6) Achieve Attack Objective	SC-15-a	SC-15(a)

Appendix B. Keyword Rules Used to Identify Controls that Support HWAM

Automated keyword searches were employed to identify SP 800-53 controls that might support each ISCM capability. Controls returned by the keyword search were then examined manually, to separate those that do support the capability (true positives) from those that do not (false positives). The specific keyword rules used for the searches are in the table below

Keyword Rule	Rationale
change control	Ensuring that devices are authorized before connection to the network Approving device hardware configurations, including consideration of the risk context
collaborative computing device	Approving device hardware configurations, including consideration of the risk context
high-risk areas	Approving device hardware configurations, including consideration of the risk context
inventory	Approving device hardware configurations, including consideration of the risk context
property	Approving device hardware configurations, including consideration of the risk context
supply chain NOT *monitoring*	Approving device hardware configurations, including consideration of the risk context
tamper resistance	Approving device hardware configurations, including consideration of the risk context
anti-counterfeit	Approving hardware with a valid supply chain that is not counterfeit
personally owned OR *non-organizationally owned systems*	Approving hardware with a valid supply chain that is not counterfeit
supply chain NOT *monitoring*	Approving hardware with a valid supply chain that is not counterfeit
thin nodes	Approving hardware with a valid supply chain that is not counterfeit
unsupport AND *system*	Approving hardware with a valid supply chain that is not counterfeit
heterogen	Using heterogeneity or diversity techniques to manage risk

Appendix C. Control Items in the Low-High Baseline that were Selected by the Keyword Search, but were Manually Determined to be False Positives

Sortable Control Item Code	SP 800-53 Control Item	Control Text	Level	Rationale for Calling a False Positive
AC-18-z-01-z	AC-18 (1)	(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION The system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Moderate	Belongs in BOUND-O
IA-03	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION Control: The system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Moderate	Involves authentication and identification of devices which is in CRED
IA-05-I	IA-5	AUTHENTICATOR MANAGEMENT Control: The organization manages system authenticators by: i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and	Low	The safeguards to protect authenticators are usually configuration settings so this is fundamentally CSM work, but risk may be more tied to CRED.
MA-02-b	MA-2	CONTROLLED MAINTENANCE Control: The organization: b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;	Low	This control item is covered under BOUND-P, which is a major protector of hardware and media
MA-02-d	MA-2	CONTROLLED MAINTENANCE Control: The organization: d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;	Low	This control item is covered under BOUND-P, which is a major protector of hardware and media

Sortable Control Item Code	SP 800-53 Control Item	Control Text	Level	Rationale for Calling a False Positive
MA-03-z-03-c	MA-3 (3)	(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (c) Retaining the equipment within the facility; or	High	This control item is covered under BOUND-P, which is a major protector of hardware and media
MA-03-z-03-d	MA-3 (3)	(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	High	This control item is covered under BOUND-P, which is a major protector of hardware and media
MP-06-z-03-z	MP-6 (3)	(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	High	This control item is covered under BOUND-P, which is a major protector of hardware and media
PE-03-a	PE-3	PHYSICAL ACCESS CONTROL Control: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];	Low	This control item is covered under BOUND-P, which is a major protector of hardware and media

Sortable Control Item Code	SP 800-53 Control Item	Control Text	Level	Rationale for Calling a False Positive
PE-03-e	PE-3	PHYSICAL ACCESS CONTROL Control: The organization: e. Secures keys, combinations, and other physical access devices;	Low	These devices are credentials, and thus assigned to CRED
PE-03-f	PE-3	PHYSICAL ACCESS CONTROL Control: The organization: f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and	Low	These devices are credentials, and thus assigned to CRED
PE-05	PE-5	PE-5 ACCESS CONTROL FOR OUTPUT DEVICES Control: The organization controls physical access to system output devices to prevent unauthorized individuals from obtaining the output.	Moderate	This control item is covered under BOUND-P, which is a major protector of hardware and media
PE-10-b	PE-10	PE-10 EMERGENCY SHUTOFF Control: The organization: b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate safe and easy access for personnel; and	Moderate	These devices are special purpose to detect and respond to contingencies. Putting the devices in place is assigned to PREP
PE-13	PE-13	PE-13 FIRE PROTECTION Control: The organization employs and maintains fire suppression and detection devices/systems for the system that are supported by an independent energy source.	Low	These devices are special purpose to detect and respond to contingencies. Putting the devices in place is assigned to PREP
PE-13-z-01-z	PE-13 (1)	(1) FIRE PROTECTION | DETECTION DEVICES / SYSTEMS The organization employs fire detection devices/systems for the system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	High	These devices are special purpose to detect and respond to contingencies. Putting the devices in place is assigned to PREP

Sortable Control Item Code	SP 800-53 Control Item	Control Text	Level	Rationale for Calling a False Positive
PE-13-z-02-z	PE-13 (2)	(2) FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS The organization employs fire suppression devices/systems for the system that provide automatic notification of any activation to Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].	High	These devices are special purpose to detect and respond to contingencies. Putting the devices in place is assigned to PREP
SC-03	SC-3	SC-3 SECURITY FUNCTION ISOLATION Control: The system isolates security functions from non-security functions.	High	Focus is on the isolation of security functions in the SWAM capability.
SC-07-c	SC-7	SC-7 BOUNDARY PROTECTION Control: The system: c. Connects to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Low	External connections are details of how that hardware/software protects the boundary are covered in BOUND N, O and P
SC-07-z-07-z	SC-7 (7)	(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES The system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	Moderate	External connections are details of how that hardware/software protects the boundary are covered in BOUND N, O and P
SI-04-c	SI-4	SI-4 SYSTEM MONITORING Control: The organization: c. Deploys monitoring devices: (i) strategically within the system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;	Low	All ISCM devices and associated requirements are covered within each capability, and data quality is assessed via defect checks Q01 through Q04.

Appendix D. Control Items Not in the Low, Moderate, or High Baselines

The following security controls items are not included in an SP 800-53 baseline and thus were not analyzed further after the keyword search:

- the Program Management (PM) Family, because the PM controls do not apply to individual systems;
- the *not selected* controls that are in other SP 800-53 families but were not assigned to a baseline; and
- the Privacy Controls.

These are listed in this appendix in case an organization wants to develop automated tests.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
AC-07-z-02-z	AC-7 (2)	(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE The system purges/wipes information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.
AC-16-z-05-z	AC-16 (5)	(5) SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES The system displays security attributes in human-readable form on each assessment object that the system transmits to output devices to identify [Assignment: organization-identified special dissemination, handling, or distribution instructions] using [Assignment: organization-identified human-readable, standard naming conventions].
AC-19-z-04-a	AC-19 (4)	(4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION The organization: (a) Prohibits the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

Sortable Control Item Code	SP 800-53 Control Item	Control Text
AC-19-z-04-b	AC-19 (4)	(4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION The organization: (b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: - Connection of unclassified mobile devices to classified systems is prohibited; - Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official; - Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and - Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.
AC-19-z-06-z	AC-19 (6)	(6) ACCESS CONTROL FOR MOBILE DEVICES | FULL DISK ENCRYPTION The organization uses full-disk encryption to protect the confidentiality of information on [Assignment: organization-defined mobile devices].
AC-19-z-07-z	AC-19 (7)	(7) ACCESS CONTROL FOR MOBILE DEVICES | CENTRAL MANAGEMENT OF MOBILE DEVICES The organization centrally manages [Assignment: organization-defined mobile devices]. Supplemental Guidance: This control enhancement applies to mobile devices that are organization-controlled and excludes portable storage media. [MAPCAT-HWAM]
AC-19-z-08-z	AC-19 (8)	(8) ACCESS CONTROL FOR MOBILE DEVICES | REMOTE PURGING OF INFORMATION The organization provides the capability to remotely purge information from [Assignment: organization-defined mobile devices].
AC-19-z-09-z	AC-19 (9)	(9) ACCESS CONTROL FOR MOBILE DEVICES | TAMPER DETECTION The organization inspects [Assignment: organization-defined mobile devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
AC-20-z-03-z	AC-20 (3)	(3) USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES The organization [Selection: restricts; prohibits] the use of non-organizationally owned systems, system components, or devices to process, store, or transmit organizational information.
AC-20-z-04-z	AC-20 (4)	(4) USE OF EXTERNAL SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES The organization prohibits the use of [Assignment: organization-defined network accessible storage devices] in external systems.
CM-03-z-03-z	CM-3 (3)	(3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION The organization employs automated mechanisms to implement changes to the current system baseline and deploys the updated baseline across the installed base.
CM-03-z-04-z	CM-3 (4)	(4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].
CM-03-z-05-z	CM-3 (5)	(5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE The system implements [Assignment: organization-defined security responses] automatically if baseline configurations are changed in an unauthorized manner.
CM-03-z-06-z	CM-3 (6)	(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.
CM-08-z-06-z	CM-8 (6)	(6) SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS The organization includes assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.
CM-08-z-07-z	CM-8 (7)	(7) SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY The organization provides a centralized repository for the inventory of system components.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
CM-08-z-08-z	CM-8 (8)	(8) SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING The organization employs automated mechanisms to support tracking of system components by geographic location.
CM-08-z-09-a	CM-8 (9)	(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS The organization: (a) Assigns [Assignment: organization-defined acquired system components] to a system; and
CM-08-z-09-b	CM-8 (9)	(9) SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS The organization: (b) Receives an acknowledgement from the system owner of this assignment.
IA-03-z-01-z	IA-3 (1)	(1) DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION The system authenticates [Assignment: organization-defined specific devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.
IA-03-z-03-a	IA-3 (3)	(3) DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION The organization: (a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and
IA-11	IA-11	RE-AUTHENTICATION Control: The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].
IR-04-z-10-z	IR-4 (10)	(10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
IR-06-z-03-z	IR-6 (3)	(3) INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN The organization provides security incident information to other organizations involved in the supply chain for systems or system components related to the incident.
MP-06-z-08-z	MP-6 (8)	(8) MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION The organization provides the capability to purge/wipe information from [Assignment: organization-defined systems, system components, or devices] either remotely or under the following conditions: [Assignment: organization-defined conditions].
PE-05-z-01-a	PE-5 (1)	(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS The organization: (a) Controls physical access to output from [Assignment: organization-defined output devices]; and
PE-05-z-01-b	PE-5 (1)	(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS The organization: (b) Ensures that only authorized individuals receive output from the device.
PE-05-z-02-a	PE-5 (2)	(2) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY The system: (a) Controls physical access to output from [Assignment: organization-defined output devices]; and
PE-05-z-02-b	PE-5 (2)	(2) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY The system: (b) Links individual identity to receipt of the output from the device.
PE-05-z-03-z	PE-5 (3)	(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES The organization marks [Assignment: organization-defined system output devices] indicating the appropriate security marking of the information permitted to be output from the device.
PM-05	PM-5	PM-5 SYSTEM INVENTORY Control: The organization develops and maintains an inventory of its systems.
SA-12-z-01-z	SA-12 (1)	(1) SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS The organization employs [Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods] for the purchase of the system, system component, or system service from suppliers.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SA-12-z-02-z	SA-12 (2)	(2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS The organization conducts a supplier review prior to entering into a contractual agreement to acquire the system, system component, or system service
SA-12-z-05-z	SA-12 (5)	(5) SUPPLY CHAIN PROTECTION | LIMITATION OF HARM The organization employs [Assignment: organization-defined security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain.
SA-12-z-07-z	SA-12 (7)	(7) SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE The organization conducts an assessment of the system, system component, or system service prior to selection, acceptance, or update.
SA-12-z-08-z	SA-12 (8)	(8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE The organization uses all-source intelligence analysis of suppliers and potential suppliers of the system, system component, or system service.
SA-12-z-09-z	SA-12 (9)	(9) SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY The organization employs [Assignment: organization-defined Operations Security (OPSEC) safeguards] in accordance with classification guides to protect supply chain-related information for the system, system component, or system service.
SA-12-z-10-z	SA-12 (10)	(10) SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED The organization employs [Assignment: organization-defined security safeguards] to validate that the system or system component received is genuine and has not been altered.
SA-12-z-11-z	SA-12 (11)	(11) SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS The organization employs [Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing] of [Assignment: organization-defined supply chain elements, processes, and actors] associated with the system, system component, or system service.
SA-12-z-12-z	SA-12 (12)	(12) SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the system, system component, or system service.
SA-12-z-13-z	SA-12 (13)	(13) SUPPLY CHAIN PROTECTION | CRITICAL SYSTEM COMPONENTS The organization employs [Assignment: organization-defined security safeguards] to ensure an adequate supply of [Assignment: organization-defined critical system components].

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SA-12-z-14-z	SA-12 (14)	(14) SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY The organization establishes and retains unique identification of [Assignment: organization-defined supply chain elements, processes, and actors] for the system, system component, or system service.
SA-12-z-15-z	SA-12 (15)	(15) SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.
SA-18	SA-18	SA-18 TAMPER RESISTANCE AND DETECTION Control: The organization implements a tamper protection program for the system, system component, or system service.
SA-18-z-01-z	SA-18 (1)	(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.
SA-18-z-02-z	SA-18 (2)	(2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF SYSTEMS, COMPONENTS, OR DEVICES The organization inspects [Assignment: organization-defined systems, system components, or devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering.
SA-19-a	SA-19	SA-19 COMPONENT AUTHENTICITY Control: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
SA-19-z-01-z	SA-19 (1)	(1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING The organization trains [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).
SA-19-z-04-z	SA-19 (4)	(4) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING The organization scans for counterfeit system components [Assignment: organization-defined frequency].

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SA-22-a	SA-22	SA-22 UNSUPPORTED SYSTEM COMPONENTS Control: The organization: a. Replaces system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
SA-22-b	SA-22	SA-22 UNSUPPORTED SYSTEM COMPONENTS Control: The organization: b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.
SA-22-z-01-z	SA-22 (1)	(1) UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT The organization provides [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]] for unsupported system components.
SC-03-z-01-z	SC-3 (1)	(1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION The system utilizes underlying hardware separation mechanisms to implement security function isolation.
SC-03-z-02-z	SC-3 (2)	(2) SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS The system isolates security functions enforcing access and information flow control from non-security functions and from other security functions.
SC-03-z-03-z	SC-3 (3)	(3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY The organization minimizes the number of non-security functions included within the isolation boundary containing security functions.
SC-03-z-04-z	SC-3 (4)	(4) SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.
SC-03-z-05-z	SC-3 (5)	(5) SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
SC-07-z-16-z	SC-7 (16)	(16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES The system prevents discovery of specific system components composing a managed interface.

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SC-15-z-01-z	SC-15 (1)	(1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT The system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.
SC-15-z-03-z	SC-15 (3)	(3) COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS The organization disables or removes collaborative computing devices from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].
SC-15-z-04-z	SC-15 (4)	(4) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS The system provides an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].
SC-25	SC-25	SC-25 THIN NODES Control: The organization employs [Assignment: organization-defined system components] with minimal functionality and information storage.
SC-29	SC-29	SC-29 HETEROGENEITY Control: The organization employs a diverse set of information technologies for [Assignment: organization-defined system components] in the implementation of the system.
SC-29-z-01-z	SC-29 (1)	(1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].
SC-37	SC-37	SC-37 OUT-OF-BAND CHANNELS Control: The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems].
SC-37-z-01-z	SC-37 (1)	(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION The organization employs [Assignment: organization-defined security safeguards] to ensure that only [Assignment: organization-defined individuals or systems] receive the [Assignment: organization-defined information, system components, or devices].

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SC-41	SC-41	SC-41 PORT AND I/O DEVICE ACCESS Control: The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined systems or system components].
SC-42-z-03-z	SC-42 (3)	(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES The organization prohibits the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems].
SE-01-a	SE-1	SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and
SE-01-b	SE-1	SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified systems containing PII.
SI-04-z-13-c	SI-4 (13)	(13) SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS The organization: (c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
SI-04-z-14-z	SI-4 (14)	(14) SYSTEM MONITORING | WIRELESS INTRUSION DETECTION The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the system.
SI-04-z-23-z	SI-4 (23)	(23) SYSTEM MONITORING | HOST-BASED DEVICES The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined system components].
SI-07-z-09-z	SI-7 (9)	(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS The system verifies the integrity of the boot process of [Assignment: organization-defined devices].

Sortable Control Item Code	SP 800-53 Control Item	Control Text
SI-07-z-10-z	SI-7 (10)	(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE The system implements [Assignment: organization-defined security safeguards] to protect the integrity of boot firmware in [Assignment: organization-defined devices].

Appendix E. HWAM-Specific Acronyms and Abbreviations

SWID – Software Identification