

NISTIR 8011

Automation Support for Security Control Assessment

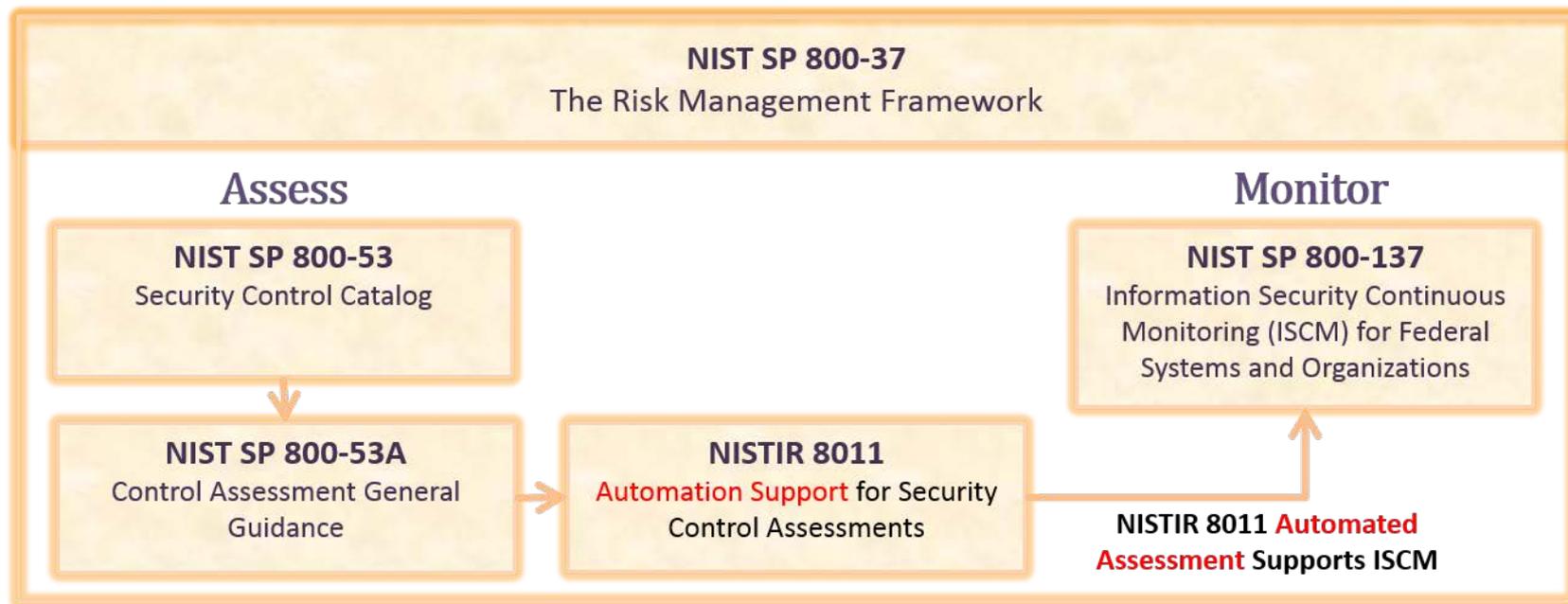
Highlights of Volume 1 (Overview) and Volume 2 (Hardware Asset Management)

Drafts of Volumes 1 and 2 are available at:

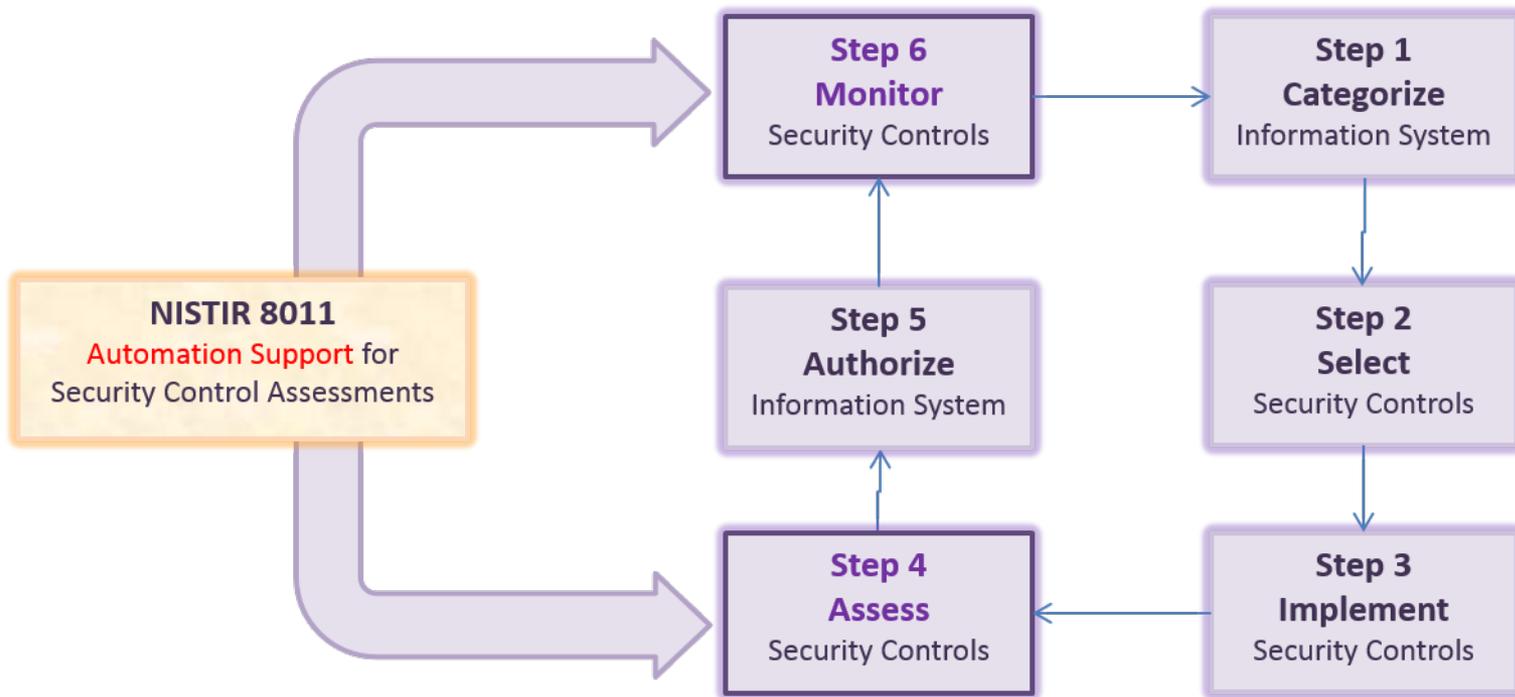
<http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8011>

Automated Assessment Foundations

The Risk Management Framework,
Information Security Continuous Monitoring,
and Automated Assessment of Security Controls

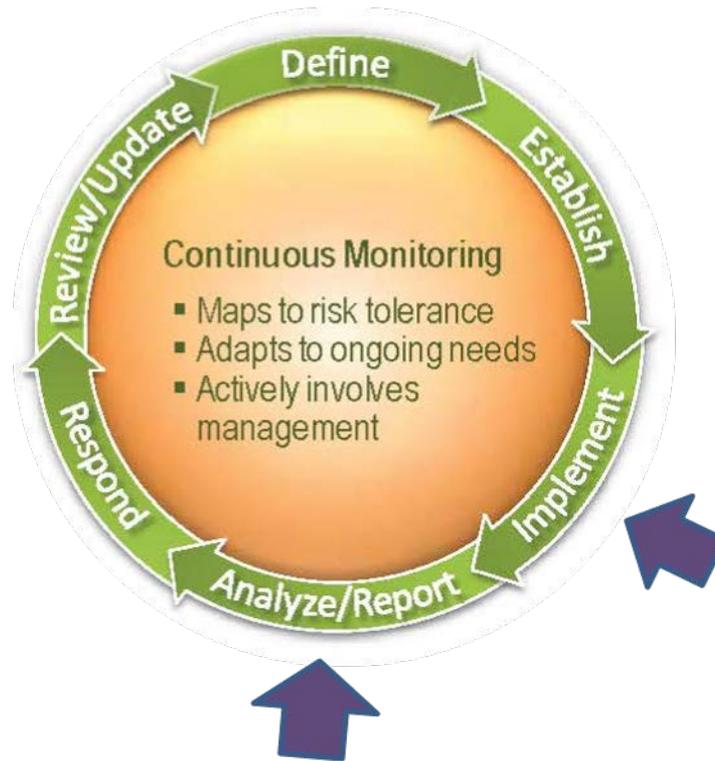


Automated Assessment in the RMF



Linkage between Monitoring and Automated Assessment

NIST SP 800-137
Information Security
Continuous Monitoring
(ISCM) for Federal
Systems and
Organizations



In the ISCM process, automated assessment encompasses the *Implement* and *Analyze and Report* steps.

Controls and Control Items

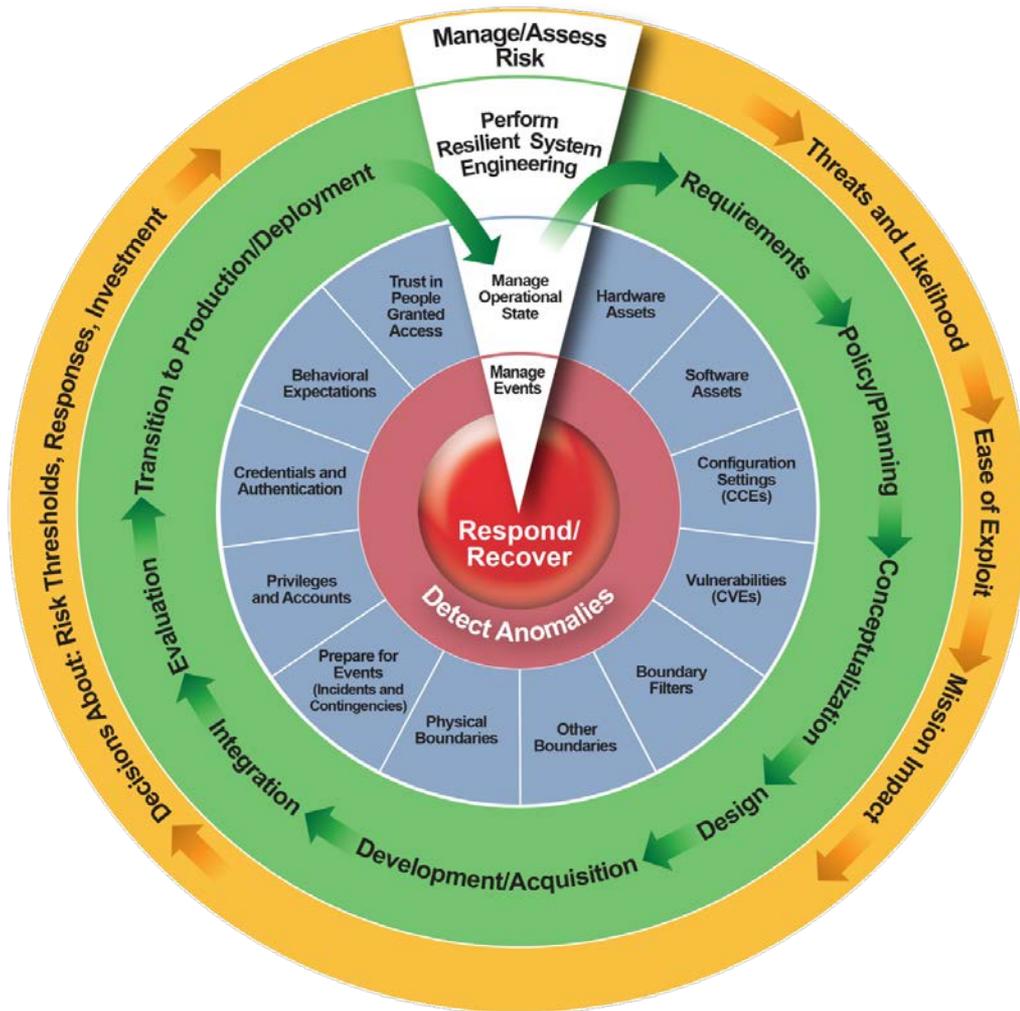
NIST SP 800-53
Security Control Catalog

NIST SP 800-53A
Assessment General
Guidance

NISTIR 8011
Automation Support for
Security Control
Assessments

- Using the security controls in SP 800-53, and referencing assessment guidance in SP 800-53A, controls are divided into more granular parts (via determination statements) to be assessed.
- The parts of the control assessed by each determination statement are called ***control items***.
- These control items are grouped into the appropriate ***ISCM security capabilities***.

ISCM Security Capabilities



ISCM Security Capabilities

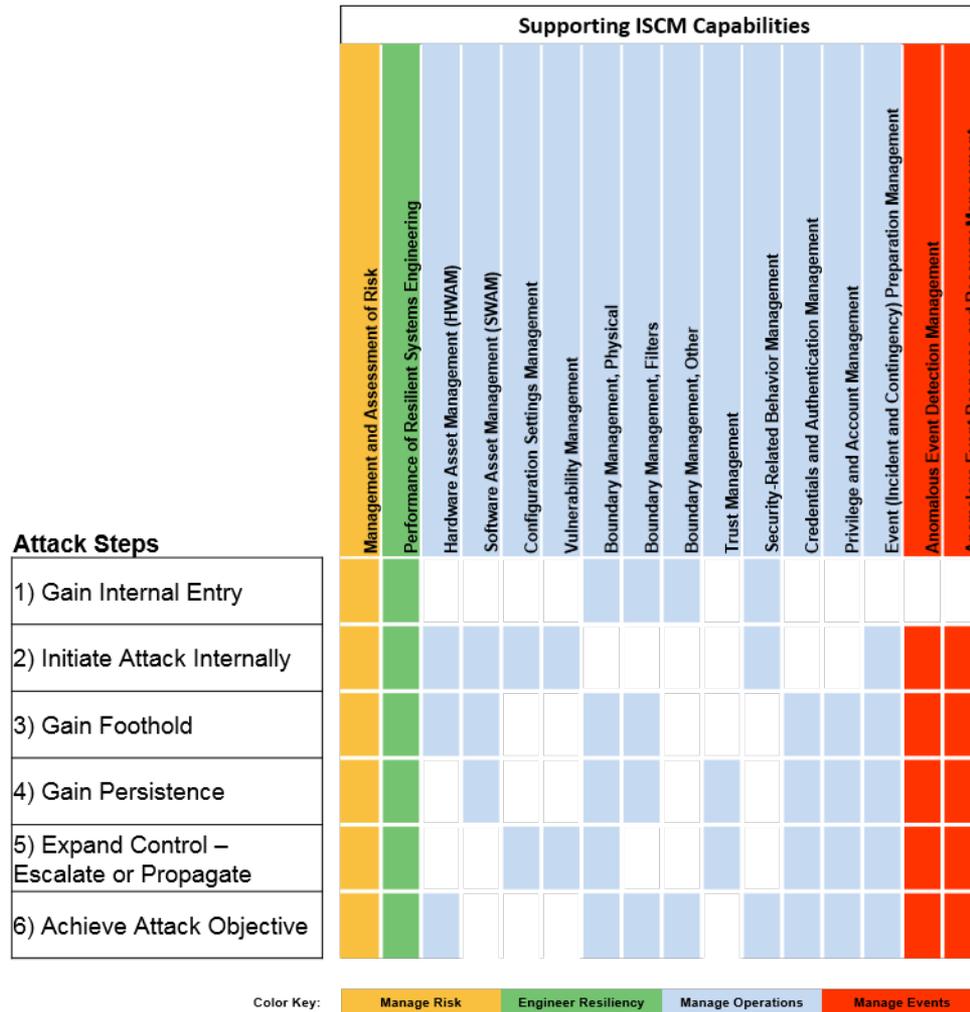
As suggested by SP 800-53A Rev 4, security *capabilities* are groups of security controls working together to support a particular *purpose*.

Attack Steps and ISCM Security Capabilities

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

The common *purpose* of each security capability is to block or limit the damage from one or more step(s) of a cybersecurity attack.

ISCM Security Capabilities Block Attack Steps



The *Test* Method of Assessment

Per SP 800-53A, assessments of the effectiveness of security controls can be done by automated *or* procedural/manual methods.

NIST SP 800-53A
Assessment General
Guidance

NISTIR 8011
Automation Support for
Security Control
Assessments

NIST SP 800-137
Information Security
Continuous Monitoring
(ISCM) for Federal
Systems and
Organizations

Method	Definition
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
Interview	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence.
Test	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

The TEST assessment method is usually the easiest and most effective to *automate*. Relying on the TEST method of assessment, NISTIR 8011 presents a way to automate assessment of a large percentage of controls, providing automation support for ISCM.

Defect Checks are Used to Confirm If a Capability is Meeting Its Purpose



Defect Checks compare actual and desired states

- NISTIR 8011 defines a set of machine-readable *defect checks* suitable for *automated assessment* of the SP 800-53 controls making up that security capability.
- Automated assessments (in the form of defect checks) are performed, using the *test assessment* method defined in SP 800-53A, by comparing a desired and actual state (or behavior).

Assessment Boundary As Entire Target Network

NIST SP 800-37

Risk Management
Framework
Supplemental Guidance
on Ongoing
Authorization

Per SP 800-37, assessments of the effectiveness of security controls are to be done for each system which has an **authorization** boundary.

NISTIR 8011

Automation Support for
Security Control
Assessments

Because it would likely be inefficient to set up ISCM tools for each system, NISTIR 8011 introduces the concept of **assessment** boundary—the whole network targeted for assessment by ISCM.

Each **authorization** boundary within an **assessment** boundary can have a separate risk report by grouping its objects for reporting.

Assembling the Assessment Package

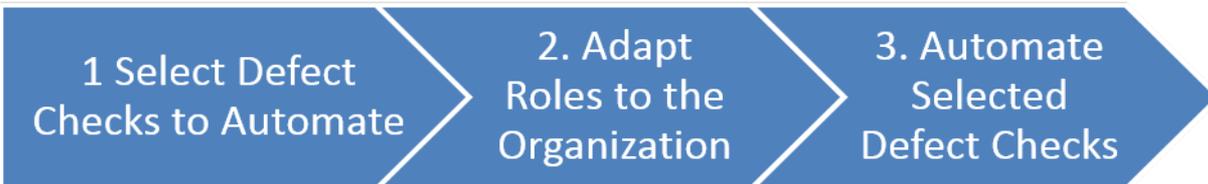
NIST SP 800-137
Information Security
Continuous Monitoring
(ISCM) for Federal
Systems and
Organizations

Required Assessment Documentation:

1. *Security Assessment Plan*

- Example provided in 8011 Overview, §6.1.
- §3.1 of each capability-specific volume contains a SAP template.
- Template can be customized to meet D/A needs.

NIST SP 800-37
Risk Management
Framework



2. *Security Assessment Results*

- *Can be provided by ISCM dashboard.*
- *Does not require paper documentation.*

Summary

NISTIR 8011 Automated Assessment

- Uses NIST Standards (SP 800-37, SP 800-53, SP 800-53A and SP 800-137) as a foundation.
- Focused on SP 800-53A **Test** assessment method
- Instead of testing individual determination statements for each security control, we are testing whether the *purposes* of the capabilities are met.
- Instead of custom-writing each SAP, can adopt template provided in the capability-specific volumes

Example: HWAM Capability

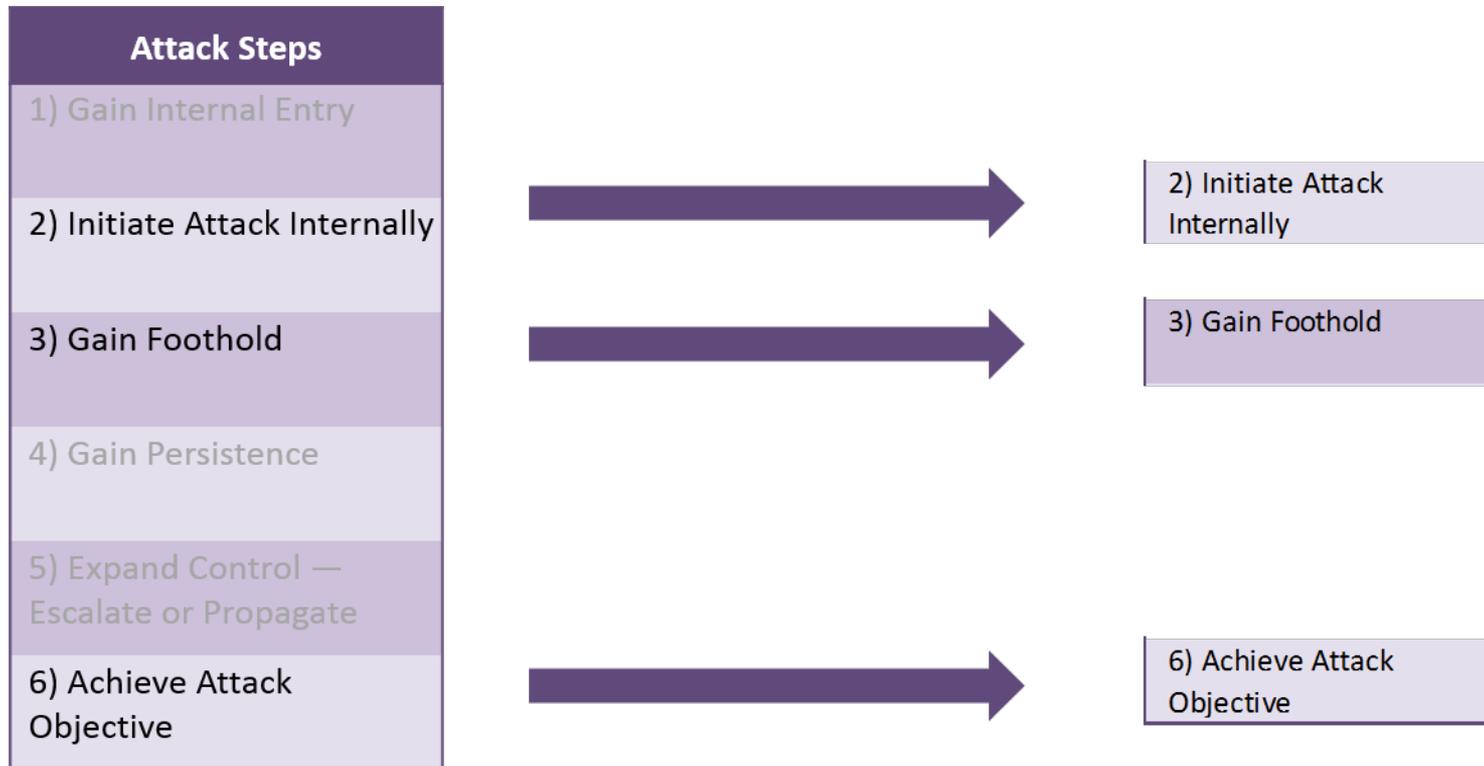
HWAM Capability Purpose:

*Manage risk created by
unmanaged devices on a
network*

Example (HWAM Capability)

Capability Purpose: Manage risk created by unmanaged devices on a network

1. The HWAM capability defends against three attack steps.



Example (HWAM Capability) cont.

Capability Purpose: Manage risk created by unmanaged devices on a network

2. The HWAM Capability breaks down into 13* parts—or *sub-capabilities*. Each sub-capability has *one defect check*.

HWAM Sub-Capabilities

Prevent unauthorized devices
Reduce number of devices without assigned device manager
Reduce exploitation of devices before removal, during use elsewhere, and after return
Reduce insider threat of unauthorized device
Reduce denial of service attacks from missing required devices
Restrict Device Ownership
Reduce unapproved suppliers and/or manufacturers
Reduce unauthorized components
Verify ongoing business need for device
Ensure required device data is collected
Ensure needed changes are approved or disapproved in a timely manner
Ensure adequate record retention
Ensure one-to-one device assignment to authorization boundary

*Note: There are also 4 sub-capabilities for data quality (see Volume 2), for a total of 17 HWAM sub-capabilities.

Example (HWAM Capability) cont.

Capability Purpose: Manage risk created by unmanaged devices on a network

		HWAM Sub-Capabilities												
Attack Steps		Prevent unauthorized devices	Reduce number of devices without assigned device manager	Reduce exploitation of devices before removal, during use elsewhere, and after return	Reduce insider threat of unauthorized device	Reduce denial of service attacks from missing required devices	Restrict Device Ownership	Reduce unapproved suppliers and/or manufacturers	Reduce unauthorized components	Verify ongoing business need for device	Ensure required device data is collected	Ensure needed changes are approved or disapproved in a timely manner	Ensure adequate record retention	Ensure one-to-one device assignment to authorization boundary
1) Gain Internal Entry														
2) Initiate Attack Internally	2) Initiate Attack Internally	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	
3) Gain Foothold	3) Gain Foothold	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
4) Gain Persistence														
5) Expand Control — Escalate or Propagate														
6) Achieve Attack Objective	6) Achieve Attack Objective	✓		✓	✓		✓	✓	✓	✓			✓	

3. Taken together, the defect checks verify that the purposes of HWAM—preventing or reducing attack steps (2), (3) and (6)—are met.

Defect Checks: A Closer Look

Each Defect Check (see, e.g., HWAM-F01 below) contains a description of the sub-capability, the purpose met by the sub-capability, and notes on how to use the defect check.

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.

Defect Check ID	Defect Check Name	Assessment Criteria Summary	Assessment Criteria Notes	Selected
HWAM-F01	Unauthorized devices	Device is In Actual State but not in Desired State	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.	Yes

Defect Checks: A Closer Look

Assessment Criteria Notes

Assessment Criteria Notes describe the mechanics of a defect check.

Assessment Criteria Notes

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.

Defect Checks: A Closer Look

Actual State

For the *Prevent Unauthorized Devices* sub-capability:

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.

Defect Checks: A Closer Look

Actual State and Desired State

For the *Prevent Unauthorized Devices* sub-capability:

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.

Defect Checks: A Closer Look

Actual State, Desired State, and Defects

For the *Prevent Unauthorized Devices* sub-capability:

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 any difference between the actual and desired state, i.e., a device in the actual state but not in the desired state (or a device in the desired state but not in the actual state).

Root Cause Analysis

In the example, if no defect is found, then it is concluded that the purpose of the *Prevent Unauthorized Devices* sub-capability is met.

However, if a defect is found, then a *root cause analysis* is required to figure out why. Three levels of analysis could be needed to find the source of the problem:

1. Determine the case-specific causes—typically whether the desired state specification was wrong or the actual state was wrong.
2. Identify which control failed.
3. Systemic analysis.

Root Cause Analysis cont.

1. Determine the case-specific causes—typically whether the *desired state specification* was wrong or the *actual state* was wrong.
 - **Example 1:** A system administrator has connected multiple devices to the production network without first getting them authorized and adding them to the authorized inventory. [*Actual state* is wrong]
 - **Example 2:** A system administrator has connected multiple devices to the production network after getting them authorized, but forgot to first add them to the authorized information system inventory. [*Desired state specification* is wrong]

Root Cause Analysis cont.

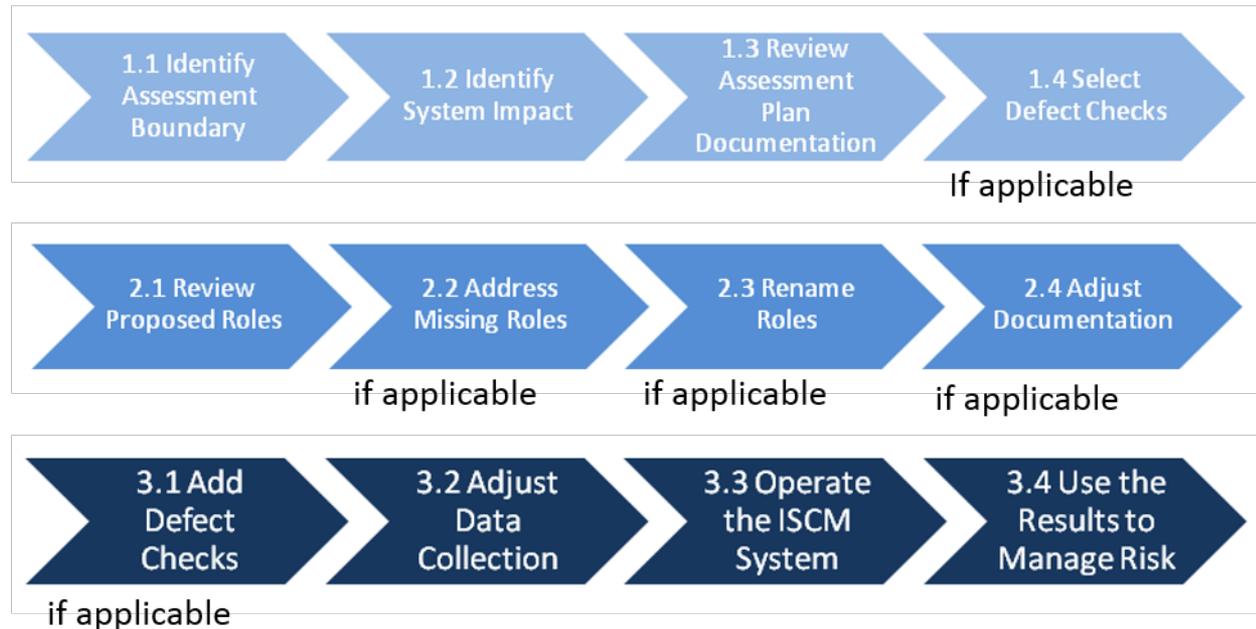
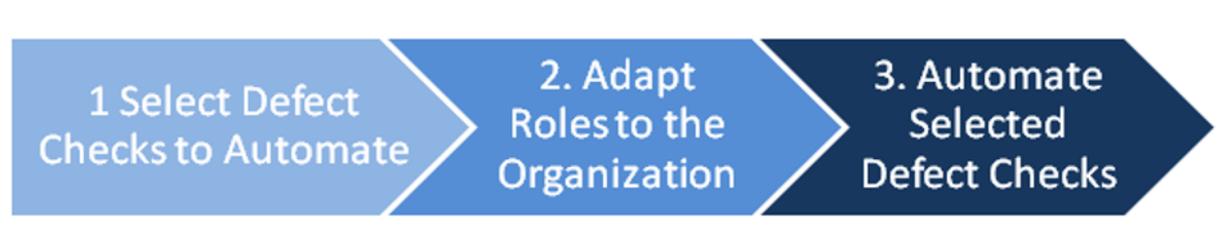
2. Identify which control failed. Use the Control-to-Defect Check Mapping table for defect check HWAM-F01. It maps to specific control items that might be causing the defect check to fail.

Defect Check ID	Baseline	NIST Control Item Code
HWAM-F01	Low	AC-19(b)
HWAM-F01	Low	CM-8(a)
HWAM-F01	Low	CM-8(b)
HWAM-F01	Low	PS-4(d)
HWAM-F01	Low	SC-15(a)
HWAM-F01	Moderate	AC-20(2)
HWAM-F01	Moderate	CM-3(b)
HWAM-F01	Moderate	CM-3(c)
HWAM-F01	Moderate	CM-3(d)
HWAM-F01	Moderate	CM-3(g)
HWAM-F01	Moderate	CM-8(1)
HWAM-F01	Moderate	CM-8(3)(b)
HWAM-F01	Moderate	MA-3(1)
HWAM-F01	High	CM-3(1)(a)
HWAM-F01	High	CM-3(1)(b)
HWAM-F01	High	CM-3(1)(d)

Root Cause Analysis cont.

- 3. Determine Systemic Causes.** Look for causes of repeated failures or engineering defects and find systemic solutions. (Example: the system administrator is unaware of operational procedures, or perhaps has too much work and is unable to keep the inventory up to date).

Implementing Automated Assessment



By the Numbers

A key feature of the 8011 approach to automated assessment is that it makes it unnecessary to test determination statements for each control individually—if the defect check for the sub-capability passes, then it is concluded that the controls supporting it are also effective.

	SP 800-53A	8011 HWAM
Control Items Selected in the Low–High Baseline	641	36
Determination Statements	TBD	43
Automatable Determination Statements	TBD	38
# of Tests (Defect Checks) required to automate assessment	TBD	17

For HWAM, then, 38 of 43 determination statements (88%) can be automated, and only 17 defect checks are required to see if the purposes of the HWAM capability are being met—a sizable reduction in required testing.

Review

NISTIR 8011 Automated Assessment

- NISTIR 8011 is:
 - Standards compliant (SP 800-37, SP 800-53, SP 800-53A and SP 800-137).
 - Focused on the **Test** assessment method.
 - Tests whether the *purposes* of security controls working together (i.e., *capabilities*) are met.
 - Green (non-paper) focus for security assessment plans, and security assessment results.
 - Automation-intensive, means less labor-intensive.
 - Automation permits timeliness—so we can shore up our defenses before attacks occur.

Questions and Answers



Additional Resources

- GSA Site
 - <http://www.gsa.gov/cdm>
- US-Cert Site
 - <http://www.us-cert.gov/cdm>
- Additional Upcoming Activities
 - March 31, 2016
 - CDM Learning Community Event
Talk with the Authors of NISTIR 8011
Time: 1:00 pm – 3:00 pm
Location: Arlington, VA
Registration Information - <https://www.us-cert.gov/cdm/training>

Survey Questions

- Please help us improve these events by answering the 5 survey questions

CUE/CPE Information

- Thanks for attending today's session!
- A generic webinar completion certificate can be downloaded from the following site:
 - <http://www.us-cert.gov/cdm>
- Hold onto the following:
- Completion certificate after filling in your name
- A copy of the email confirmation showing you registered for the webinar

Contact Information

*THANK YOU FOR
ATTENDING OUR WEBINAR.*

Contact: cdm.fnr@hq.dhs.gov