Continuous Diagnostics and Mitigation

Automation Support for Security Control Assessments

Learning Community Event

March 31, 2016

Homeland Security

Federal Network Resilience

Table of Contents

I. Introduction

Since 2011, Federal Information Security Management Act (FISMA) guidance has stated that Information Security Continuous Monitoring (ISCM) could replace triennial manual assessment:

> *An ISCM program is established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls. Organizational officials collect and analyze the data regularly and as often as needed to manage risk as appropriate for each organizational tier. This process involves the entire organization, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual systems in support of the organization's core missions and business processes. Subsequently, determinations are made from an organizational perspective on whether to conduct mitigation activities or to reject, transfer, or accept risk… Organization-wide monitoring cannot be efficiently achieved through manual processes alone or through automated processes alone. Where manual processes are used, the processes are repeatable and verifiable to enable consistent implementation. Automated processes, including the use of automated support tools (e.g., vulnerability scanning tools, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient.*
>
> *Dempsey, Chawla, Johnson, Johnston, Jones, Orebaugh, Scholl, and Stine*
> *NIST Special Publication 800-137, 2011, 1*

National Institute of Standards and Technology Interagency Report (NISTIR) 8011: *Automation Support for Security Control Assessments, Volumes 1 and 2* is a joint effort between NIST and the Department of Homeland Security (DHS) to provide an operational approach for automating security control assessments to facilitate ISCM, ongoing assessment, and ongoing security authorization consistent with NIST SP 800-37, the Risk Management Framework (RMF), as well as guidance in NIST Security Publications (SPs) 800-53, 800-53A and 800-137.

The DHS Federal Network Resilience (FNR) Division Learning Program hosted a virtual Learning Community Event (LCE) on March 31, 2016, and invited the authors of NISTIR 8011 Volume 1 and Volume 2 to participate in a panel discussion to discuss the key concepts and respond to questions from participants.

The panelists included:

- Kelley Dempsey, National Institute of Standards and Technology
- Paul Eavy, Department of Homeland Security
- George Moore, Johns Hopkins University Applied Physics Laboratory

II. Meeting Summary

A. Key Concepts

During the learning event, the panelists focused on NISTIR 8011: *Automation Support for Security Control Assessments, Volumes 1 and 2*. The following section summarizes key concepts selected from the volumes.

Volume 1: Overview (page # references in parentheses)

Summary of Security Control Assessment Automation: Security threats are materializing at an accelerated pace. Automation—versus manual procedural testing—of security assessments can provide more timely alerts of security control defects. More timely alerts also can give organizations a better chance to fix defects before the vulnerabilities are exploited. Automated security control assessment can also be less resource-intensive than manual procedural testing, allowing any realized savings to free up resources for other activities—perhaps allowing organizations to invest in additional safeguards or countermeasures, or to respond to security defects and incidents in a more timely manner. (p. 1)

Key Terms. NISTIR 8011 Volume 1 contains an overview of one method for automation of security control assessments. Important terms used to describe the method are *Control Items*, *Capabilities*, and *Purposes*, described below:

- **Controls and Control Items**. Using the security *controls* defined in SP 800-53, and the guidance for assessment of those controls prepared in SP 800-53A, determination statements are parsed to break the controls into assessable parts. The parts of the control assessed by each determination statement are called *control items*.
- **ISCM Security Capabilities**. ISCM security *capabilities* are groups of security control items working together to support a particular *purpose*.
- **Capability Purposes**. The common *purpose* of each security capability is to block or limit the damage from one or more step(s) of a cybersecurity *attack*.
- **Cybersecurity Attack Steps**. The attack step model used by NISTIR 8011 describes the attack steps for which specific *defensive* actions are required. Those attack steps are:
    1. Gain internal entry.
    2. Initiate attack internally.
    3. Gain foothold.
    4. Gain persistence.
    5. Expand control — Escalate or propagate.
    6. Achieve Attack Objective.
- **Sub-capabilities and Purposes**. Capabilities break down into parts—called *sub-capabilities* in NISTIR 8011. Each sub-capability does its part limiting the damage from

an attack—defending against one or more of the attack steps against which the overall capability defends.

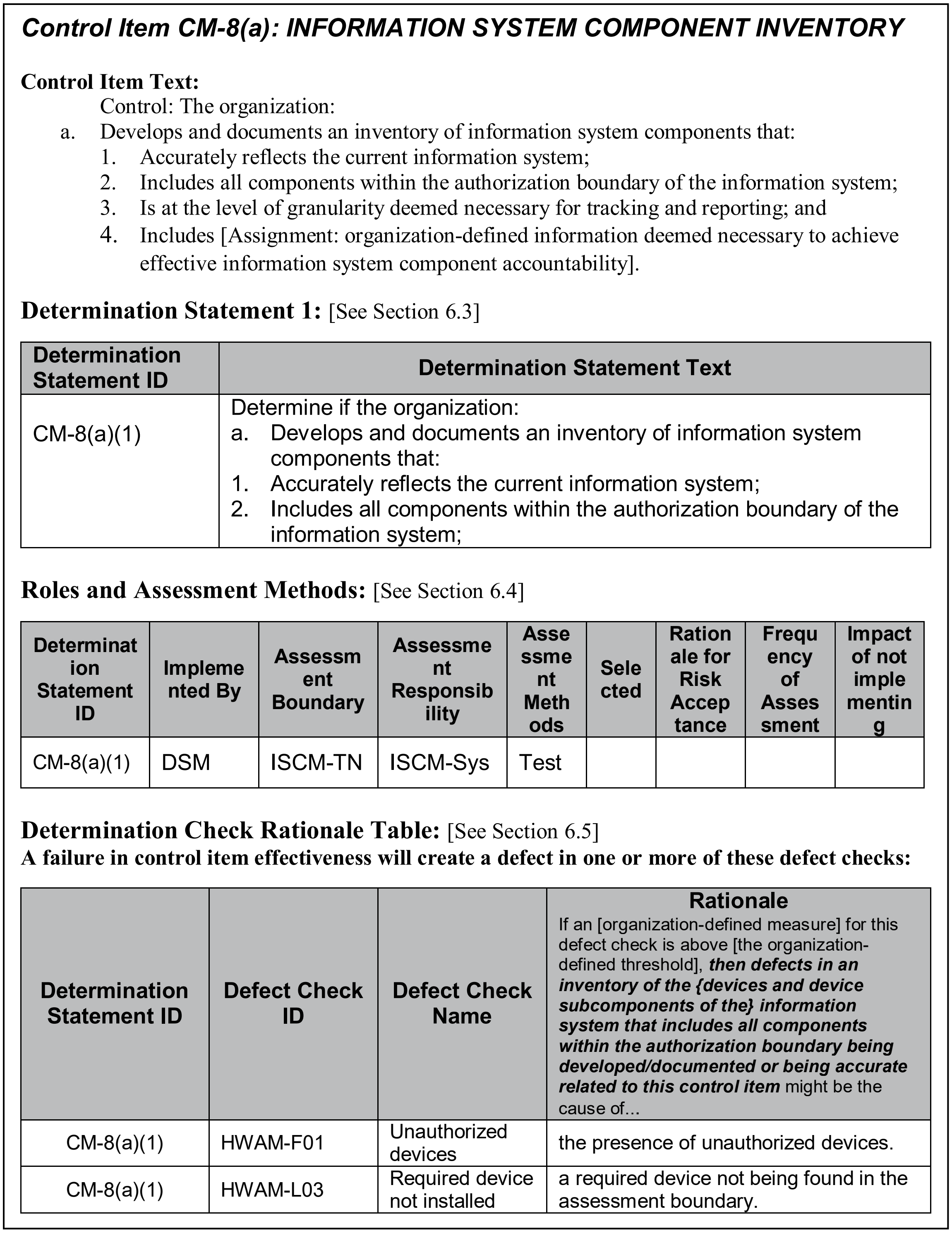
- **Defect Check:** Each sub-capability has one *defect check*—which verifies that the purpose of the sub-capability is met. A defect check works by comparing the desired state and the actual state of a control or set of controls: If there is no difference, then there is no defect; if there is a difference, then at least one security is not effective, and root cause analysis is performed to determine which control is ineffective.

Transitioning from a Manual Checklist to an Automated Approach: The transition from manual to automated security control assessment requires time and effort to devise, prepare, and implement (1) a data collection system that supports automated security control assessments, and (2) an ISCM dashboard to visualize assessment results. Resources are also required to modify and update the assessment process. An organizational-level dashboard collects data from a collection system and shows detailed object-level data and object-level defects to organizationally authorized personnel, who use the information to locate and then mitigate defects. NISTIR 8011 supports the transition to automated security control assessments by providing a customizable security assessment plan that is consistent with NIST guidance. (Volume 1, p. 1)

Template for Assessment Plan Documentation: Figure 1 provides an example template for automated reporting. See §6, Assessment Plan Documentation for an overview (Volume 1, p. 60), and see §3, HWAM Security Assessment Plan Documentation Template, for the complete details (Volume 2, p. 14).

Root cause analysis. If a control fails, the agency would need to conduct analysis to identify the root cause of the failure. Root cause analysis is often needed to determine which control or control item has failed when a defect is found within a capability. It operates on the logical flow of cause to effect from control items to the security result that is the objective of a security capability. The desired security result is to make attack scenarios and/or exploits more difficult to conduct by reducing the number of defects that can be exploited or reducing the likelihood that defects will be exploited. Desired security results will be identified for each capability in the subsequent volumes of this NISTIR. (Volume 1, p. 60)

ISCM Strategy: NISTIR 8011 is consistent with NIST guidance, specifically SP 800-37, SP 800-137, SP 800-53, and SP 800-53A. While its usage is not required, it is an acceptable method for automating security control assessments. The authors invite participants in automated control assessment to share the approaches they find successful with the NIST authors.



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

Control Item Text:

Control: The organization:

a. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information 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 information system component accountability].

Determination Statement 1: [See Section 6.3]

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

Roles and Assessment Methods: [See Section 6.4]

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				

Determination Check Rationale Table: [See Section 6.5]

A failure in control item effectiveness will create a defect in one or more of these 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} information 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.

Figure 1.—Example of a Security Assessment Plan Narrative (Courtesy of NIST)

Volume 2: Hardware Asset Management (page # references in parentheses)

Hardware Devices. Hardware devices are the objects directly managed and assessed by the Hardware Asset Management (HWAM) capability. Note that hardware that cannot be attacked independently is not included. For example, remote attacks affect a device through its Internet Protocol (IP) and cannot attack a computer mouse independently. Therefore, a component such as a computer mouse is not considered to be a separate device. The following elements are defined in the HWAM architecture and Concept of Operations (COP):

- IP addressable hardware (or equivalent);
- Removable hardware of security interest such as USB devices (USB thumb drives or USB hard drives); and
- Virtual Devices included in hardware assets as devices. (Volume 2, p. 5)

Purpose of HWAM Capability. HWAM blocks or delays three types of attack steps:

- **Initiate Attack Internally:** The attacker is inside the boundary and initiates attack on some object internally. Examples include: User opens spear phishing email or clicks on attachment; user installs unauthorized software or hardware; unauthorized personnel gains physical access to restricted facility.
- **Gain Foothold:** The attacker has gained entry to the 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.
- **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 personally identifiable information (PII). (Volume 2, pp. 2–3)

HWAM Sub-capabilities. The pieces at the heart of the HWAM capability are the *HWAM sub-capabilities*. Listed below are the names and corresponding purposes of the HWAM sub-capabilities.

- **Prevent unauthorized devices**. Prevent or reduce the presence of unauthorized devices, thus reducing the number of potentially malicious or high-risk devices.
- **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).
- **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.

- **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.
- **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.
- **Restrict Device Ownership**. Ensure that devices not owned by the organization are not connected in the assessment boundary, or that they are authorized for connection only in accordance with organizationally-defined restrictions.
- **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).
- **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.
- **Verify ongoing business need for device**. Require periodic and/or event driven consideration of whether a device is still needed for information system functionality to fulfill mission requirements in support of least functionality.
- **Ensure required device data is collected**. Ensure that data required to assess risk are collected. These data may relate to other than a HWAM defect but may need to be collected by the HWAM sensor. For example, devices with inadequate memory to support basic OS and defensive security components may need to be detected as defects.
- **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.
- **Ensure adequate record retention**. Ensure adequate historical records of HWAM ISCM data are kept in support of forensics and other risk management activities.
- **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 assessment boundary.

HWAM Defect Checks. For each sub-capability, there is one defect check (documented for HWAM in the assessment narrative of Volume 2). Individually, the defect checks verify that the purpose of the sub-capability is being met. Taken together, the defect checks for HWAM verify that the purposes of HWAM—preventing or reducing attack steps [2], [3] and [6] (i.e., [2] Initiate Attack Internally; [3] Gain Foothold; and [6] Achieve Attack Objective) when going through hardware—are met.

B. Document Timeline

NISTIR Volumes 1 and 2 should be finalized during Q4FY16. Additional volumes are in-progress, and the expectation is that Volume 3 will be released for public comment in Q4FY16. All volumes should be released within the next two years.

C. Additional Resources

These resources are intended to help agencies implement automated security control assessments:

- **CDM Bits and Bytes Email Newsletter.** Provides weekly CDM tips, information for upcoming CDM events, and updates on new CDM resources. Register here: https://www.us-cert.gov/cdm/home.

- **Federal Risk Scoring Sub-Working Group.** Develops risk scoring for the CDM program, and is looking for input from cybersecurity professionals. Contact cdm.fnr@hq.dhs.gov for more information.

- **Federal Security Systems Management Forum.** Promotes the sharing of information system security information among Federal agencies. Participation is limited to Federal Government employees who help manage their organization's information system security program. Click here to read more about the forum: http://csrc.nist.gov/groups/SMA/forum/index.html. Email sec-forum@nist.gov with your name, title, agency, email address, mailing address, telephone number, and confirmation that you are a Federal employee to join the listserv.

- **National Cybersecurity Workforce Framework.** Provides educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize, think, and talk about cybersecurity work, including what is required of the cybersecurity workforce: https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework.

- **NIST Computer Security Resource Center.** Provides information on NIST publications: http://csrc.nist.gov/. Click here to view the initial public draft of NISTIR 8011: http://csrc.nist.gov/publications/PubsDrafts.html.

- **US-CERT Portal.** Helps government users share threat information: https://portal.us-cert.gov/.

- **US-CERT Website.** Provides additional CDM information, including CDM resources, event information, and meeting summaries: https://www.us-cert.gov/.

Submit any questions, ideas for future meetings, or comments to cdmlearning@hq.dhs.gov.

III. **Appendices**

A. Meeting Agenda

TIME	ACTIVITY
1:00-1:10	**Agenda Review and Introduction** • Overview of the session and rules of engagement
1:10-1:20	**Panelist Self-Introductions** ***Kelley Dempsey,*** *NIST* ***Paul Eavy,*** *DHS FNR* ***George Moore,*** *JHU APL*
1:20-2:45	**Question and Answer with Panelists** • Pre-defined questions from the moderator • Questions from the audience
2:45-2:55	**Closing Statements from the Panelists** – Moderator summarizes the meeting and asks each panelist to provide their closing thoughts.
2:55-3:00	**Wrap-up and Thank You** ***Patrick White,*** *Nexight Group LLC*

B. References

Dempsey, Kelley, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine. “NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.” Gaithersburg, MD: National Institute of Standards and Technology. September 2011. http://csrc.nist.gov/publications/PubsSPs.html#SP 800

Dempsey, Kelley, Paul Eavy, and George Moore. “Draft NISTIR 8011: Automation Support for Security Control Assessments, Volume 1: Overview.” Gaithersburg, MD: National Institute of Standards and Technology. Released for comment February 2016. http://csrc.nist.gov/publications/drafts/nistir-8011/nistir_8011_ipd-draft_vol1_overview.pdf.

Dempsey, Kelley, Paul Eavy, and George Moore. “Draft NISTIR 8011: Automation Support for Security Control Assessments, Volume 2: Hardware Asset Management.” Gaithersburg, MD: National Institute of Standards and Technology. Released for comment February 2016. http://csrc.nist.gov/publications/drafts/nistir-8011/nistir_8011_ipd-draft_vol2-hwam.pdf.