NIST Cybersecurity White Paper
NIST CSWP 30

# Automation Support for Control Assessments

*Project Update and Vision*


Eduardo Takamura
Jeremy Licata
Victoria Pillitteri
*Computer Security Division*
*Information Technology Laboratory*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.30

December 6, 2023

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

**NIST Technical Series Policies**
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

**Publication History**
Approved by the NIST Editorial Review Board on 2023-11-27

**How to Cite this NIST Technical Series Publication:**
Takamura E, Licata J, Pillitteri V (2023) Automation Support for Control Assessments: Project Update and Vision. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 30. https://doi.org/10.6028/NIST.CSWP.30

**Author ORCID iDs**
Eduardo Takamura: 0000-0002-9978-9050
Jeremy Licata: 0000-0001-8793-5471
Victoria Pillitteri: 0000-0002-7446-7506

**Contact Information**
8011comments@list.nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

## Abstract

In 2017, the National Institute of Standards and Technology (NIST) published a methodology for supporting the automation of Special Publication (SP) 800-53 control assessments in the form of Interagency Report (IR) 8011. IR 8011 is a multi-volume series that starts with an overview of the methodology (volume 1) and provides guidance and specifications for automating the assessment of controls that support specific information security continuous monitoring security capabilities, one volume per capability. Four volumes have been released so far, and more volumes are in development. In 2023, the NIST Risk Management Framework project — responsible for the development and maintenance of Federal Information Security Modernization Act (FISMA)-supporting technical publications and the IR 8011 series — performed an internal review of the IR 8011 project. This review yielded results that offered the IR 8011 Development Team opportunities to improve the current IR 8011 methodology, facilitate its adoption, and more. This cybersecurity white paper summarizes some of the findings from this internal review.

## Keywords

actual state; assessment; attack; automation; capability; community of interest; CoI; control; control assessment; control item; defect; defect check; defend; desired state specification; FISMA; information security continuous monitoring; ISCM; methodology; monitoring; ongoing assessment; privacy; risk; risk management; security; security automation.

## Table of Contents



## List of Tables



## List of Figures

## Acknowledgments

The authors would like to thank Kelley Dempsey, Paul Eavy, George Moore, and all past collaborators for their historical contributions to the IR 8011 project, including helping establish the foundation on which IR 8011 is built; Jim Foti for layout, formatting, and styling guidance and support; Isabel Van Wyk for copy editing this publication; and Ned Goren and Allen Wilkinson for reviewing this paper.

## Terminology and Conventions

Key concepts are introduced and described in IR 8011, Volume 1 [2], including terms such as *desired* and *actual state*, *defect check*, and *attack* and *block steps*. One important term that is used throughout the IR 8011 series is *capability*, specifically *security capability*. NIST publications, including those that support the NIST Risk Management Framework (RMF)[1], refer to *capability* to express the potential to achieve an objective, whether it is a security objective or a privacy objective. In many cases, this potential is provided through the implementation of controls. In the context of IR 8011, the term *capability* refers to the potential provided by a *set of controls* to achieve a common objective. The objective in this case is the defense against a possible but specific attack that can compromise the confidentiality, integrity, and availability of information including private information. Meeting this objective means having a *functional capability*. This functional capability is associated with the defense capability of a system or organization against an attack or attack vector and is further broken down into *sub-capabilities*. Sub-capabilities facilitate the automation of control assessments that focus on the testable parts of the controls. The actual tests are what IR 8011 refers to as *defect checks*.

The premise of IR 8011 is *supporting* the automation of control assessments, which in turn can enable information security continuous monitoring (ISCM) [2], ongoing assessment, and ongoing authorization.[3] The term *ISCM security capability* will be maintained in a future revision to IR 8011, Volume 1 [2] as a legacy term. A proposed updated methodology for IR 8011 will be disassociated from ISCM in order to support other control-based frameworks and provide additional implementation options for its operationalization. New volumes will continue to be based on SP 800-53 controls, and each volume will be dedicated to a specific ISCM security capability.

When referring to the individual documents or collection of volumes comprising the series, the authors use the terms “IR 8011,” “IR 8011 series,” or simply “the Series.” When referring to a specific volume, the authors use “IR 8011vN,” where “N” is the volume number. For example, NIST IR 8011, Volume 2 [3] can be expressed as “IR 8011v2,” and NIST IR 8011, Volume 4 [5] can be expressed as “IR 8011v4.” When referring to the NIST project responsible for the development and maintenance of the IR 8011 volumes, the authors use “IR 8011 Project.” “IR 8011 Team” refers to the “IR 8011 Development Team,” which includes members of the NIST RMF Team.

[1] The NIST Risk Management Framework (RMF) is described in NIST Special Publication 800-37 [5].
[2] For more on continuous monitoring and continuous monitoring strategy, see SP 800-37 [5] and SP 800-137 [1].
[3] For more on ongoing assessments and ongoing authorization, see SP 800-37 [5].

In **Sec. 4**, the term “interested party” is used in lieu of the term “stakeholder” because involved parties may or may not have a stake in IR 8011 (e.g., development, implementation/adoption, support).

Finally, when automation is not explicit in reference to control testing, there is an assumption that such testing is automated or at least semi-automated. IR 8011 is not about automating the *implementation* of security and privacy controls. Rather, it is about supporting the *assessment* of controls using automation.

## 1. Introduction

NIST Interagency Report (IR) 8011, *Automation Support for Security Control Assessments*, is a multi-volume series that provides a blueprint for supporting automated control assessments. It proposes an approach for creating specific tests (denominated *defect checks*) that can be executed using automation to help verify that controls are in place and operating as expected. IR 8011 supports the NIST Risk Management Framework (RMF) — the methodology for managing security and privacy risks that is described in NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [5]. It expands on the guidance provided by SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations* [9], which is the guide for assessing SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [7]. IR 8011 was developed to ultimately support information security continuous monitoring (ISCM) activities[4], including ongoing assessments and ongoing authorizations.[5]

The first volume in the IR 8011 series (*Overview*) establishes the approach and organization of the methodology that is followed and adhered to by subsequent volumes. Both the *Overview* volume (8011v1 [2]) and the first capability-specific volume (*Hardware Asset Management* [3]) were published in 2017. The second capability-specific volume (*Software Asset Management* [4]) was released in 2018, and the third capability-specific volume (*Software Vulnerability Management* [6]) was published in 2020. NIST updated SP 800-53 [7] in 2020 and SP 800-53A [9] in 2022.

The NIST RMF Project performed a full review of the IR 8011 series in preparation for aligning the IR 8011 publications with the major revisions to key RMF publications, namely SP 800-53 [7], SP 800-53B [8], and SP 800-53A [9]. In the process, the Team identified a number of opportunities for improving IR 8011, ranging from an updated IR 8011 methodology and guidance to the potential for the operationalization of IR 8011.

This paper summarizes some of the findings from this internal review of the IR 8011 Project. It provides a glimpse of what is coming next and updates the IR 8011 development and maintenance roadmap. The authors recommend reviewing IR 8011v1 prior to proceeding. The internal review conducted in 2023 considered past analysis work and previously obtained feedback from the public to identify opportunities for improvement to the Series. Most of the public comments were received in response to the IR 8011v4 [5] draft comments and the February 2023 call for adoption feedback [9].

[4] See SP 800-137 [1] for more information on developing a continuous monitoring strategy and on implementing a continuous monitoring program.
[5] See SP 800-37 [4] for more information on the NIST RMF, RMF steps, ISCM, ongoing assessments, and ongoing authorizations.

## 2. Updates to the IR 8011 Methodology

Three updates to the IR 8011 methodology are planned:

1. Restructuring the IR 8011 workflow to improve readability and make it easier to understand.
2. Expanding the scope of the keyword search function to include additional control descriptors (e.g., the "Discussion" text of each control).
3. Abstracting the security framework so that the model can be used with any control-based (or requirement-based) framework, which also supports the development of defect checks for any control/control family, not just for ISCM security capabilities (see **Sec. 2.3**).

   Note: the abstraction of the security framework is only intended to promote wider adoption of the methodology for the development of defect checks. For IR 8011, the development of new volumes will continue to be based on the SP 800-53 control catalog, focusing on a given ISCM security capability – one capability per volume – as designed.

### 2.1. Logical Workflow[6]

Understanding the methodology is key to adoption, so the order in which the IR 8011 elements are presented in IR 8011v1 [2] will be updated to improve readability. For example, the workflow will be presented in a staged manner with a description of each stage (including individual stages for each abstraction layer in the methodology) and what occurs in them, similar to phases or steps being described in a process.

As a preview, the original IR 8011 methodology will be further explained using the following updated workflow:

1. For each ISCM security capability, identify potential *attacks/attack vectors*.[7]
2. For each attack/attack vector, determine the necessary defense. This will become the *functional capability*[8] (i.e., the security capability[9] to defend against attacks).
3. For each defense (referred to as "block or delay" in IR 8011v1 [2]), determine what can be tested via automated means. These will become *sub-capabilities*.[10]
4. For each sub-capability, specify the desired states.[11] These will become *control items*.
5. For each desired state specification, determine how an actual state can be tested. These will become *defect checks*.

[6] This section covers the original (legacy) IR 8011 methodology presented by IR 8011v1 [2] (2017).
[7] This is a reference to the attack step abstraction layer (IR 8011v1 [1], Sec. 3).
[8] This is a reference to the functional capability abstraction layer (IR 8011v1 [1], Sec. 3)
[9] Not to confuse with "ISCM security capability."
[10] This is a reference to the sub-capability abstraction layer (IR 8011v1 [1], Sec. 3)
[11] The desired states should include any organization-defined parameter (ODP) values.

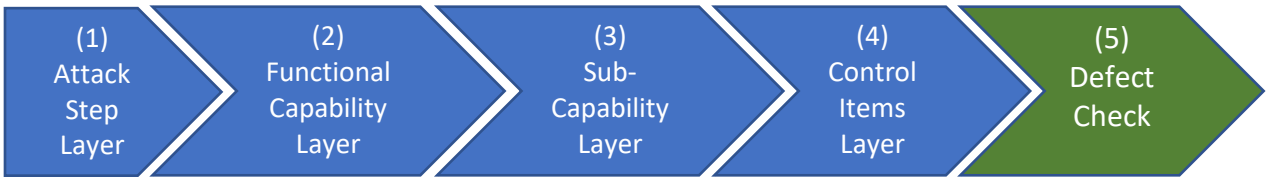


**Fig. 1. IR 8011 methodology workflow summarized as security capability abstraction layers**

**Figure 1** lays out the four security capability abstraction layers (discussed in Sec. 3 of IR 8011, Volume 1 [2]) followed by the defect check component, which refers to the necessary tests that can be automated in support of an assessment against an ISCM security capability implementation.

## 2.2. Keyword Searches

One of the main goals of IR 8011 is the development of defect checks. The defect check development process in the IR 8011 methodology relies heavily on searches of a control source (i.e., control catalog) using specific keywords to identify controls. If the appropriate keywords are not used, the correct controls may not be found.[12] Control catalogs (i.e., the source) may have different structures with both normative and informative content.

The methodology will be updated to expand the scope of the keyword search to include SP 800-53 [7] control discussion text in addition to the control title and description. Additional guidance will also be included regarding the use of synonyms for keyword searches to avoid limiting searches to a single variation of a word.

Finally, IR 8011v1 [2] will include a discussion on the limitation of the current keyword search process, a limitation that one day may be addressed by artificial intelligence to enhance and improve the control search process.

## 2.3. Security Framework Abstraction

The original IR 8011 methodology described in IR 8011v1 [2] focuses on the development of defect checks in support of ISCM security capabilities[13], and each volume in the IR 8011 series is dedicated to a single ISCM security capability. Thus, the defect checks in each IR 8011 volume are derived from the identified potential attacks/attack vectors against an ISCM security capability (see **Fig. 1** above for the methodology workflow).

The IR 8011 methodology is being slightly modified and adapted to support the development of defect checks for any control, control item, or control family, and not just for a specific ISCM security capability. This updated methodology will be described in the next revision to IR 8011v1. **Figure 2** provides a preview of the updated methodology workflow highlighting the

[12] As a result, false positives and false negatives may occur.
[13] IR 8011v1 [2] enumerates all ISCM security capabilities that will be addressed by IR 8011.

stages and the outcomes of each stage of the model. **Table 1** further describes the output of each stage of the workflow.

This update to the IR 8011 methodology will not affect the maintenance of existing volumes in the Series or the development of new volumes, which will continue to focus on defect checks for specific ISCM security capabilities utilizing the NIST SP 800-53 control catalog.

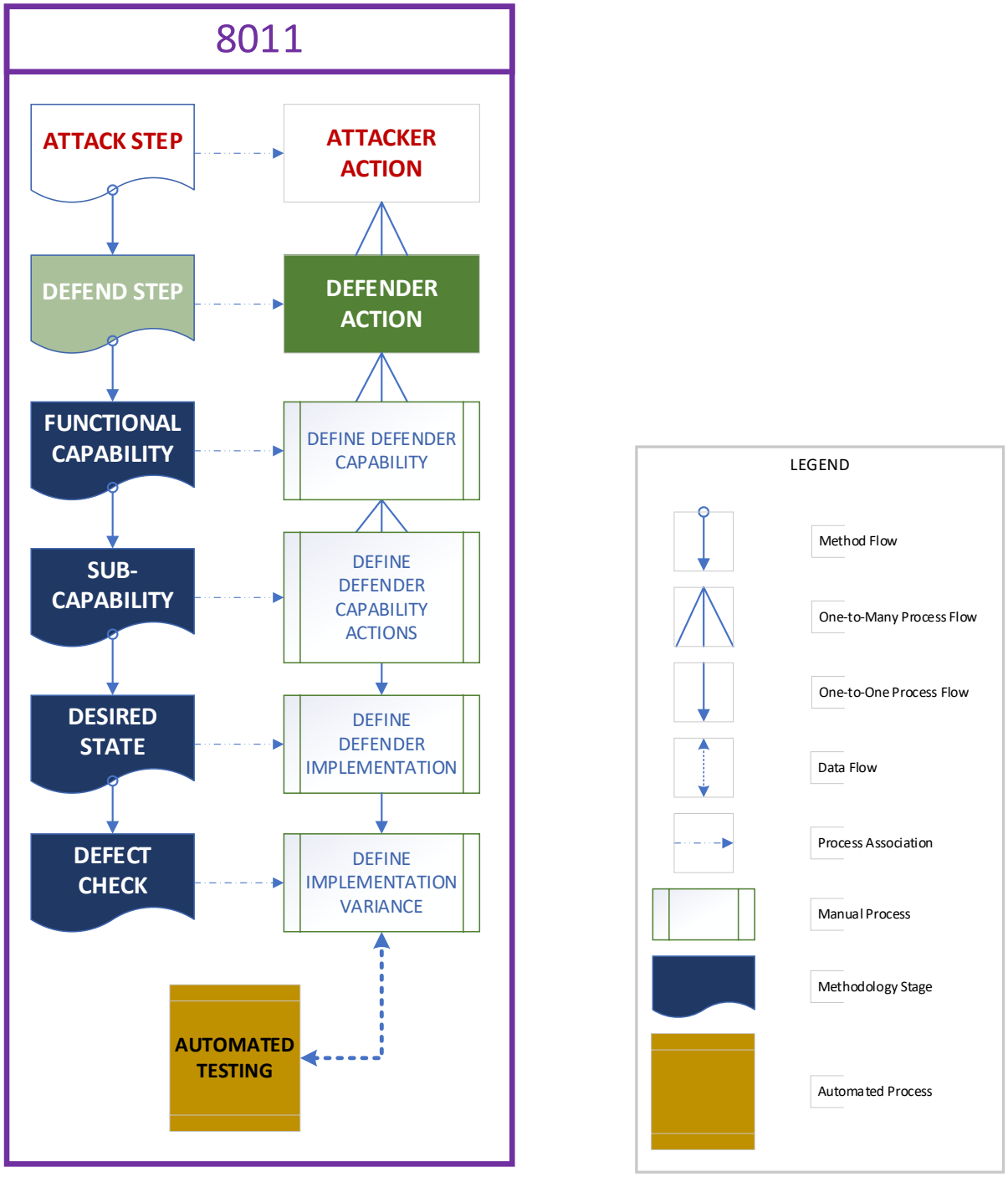


**Fig. 2. Updated IR 8011 methodology workflow with output**

A summary of the output of each stage in the methodology is provided in **Table 1**.

**Table 1. Updated IR 8011 methodology workflow output summary**

| STAGE | OUTPUT | OUTPUT SUMMARY |
|---|---|---|
| **Attack Step** | Attacker Action | Understanding the threat, the exploitable vulnerability, and the potential threat vector(s) that can be used to exploit the vulnerability |
| **Defend Step** | Defender Action | Understanding the expected ability to detect an attack and to protect the organization, the system, or the component being attacked or targeted |
| **Functional Capability** | Define Defender Functional Capability | Identifying functional capabilities to support the defender action(s) |
| **Sub-Capability** | Define Defender Capability Actions | Defining specific actions to support risk mitigation efforts for each functional capability |
| **Desired State** | Define Defender Implementation | Determining the *desired state*, including any acceptable parameters or thresholds for each defender capability action |
| **Defect Check** | Define Implementation Variance | Understanding that a *defect* that can occur when the *actual state* operates outside of the bounds of the *desired state* of the implementation |

## 2.4. Support for Other Control-Based Frameworks

Although originally written to support the NIST RMF with the SP 800-53 [7] control catalog, the IR 8011 methodology can be framework-agnostic, meaning that it can support any control-based framework (or requirement-based framework). IR 8011v1 [2] will be updated to show an abstraction of the security framework from the defect check development process. To illustrate, **Fig. 2** provides a preview of the updated methodology with an abstracted security framework. It also shows changes that will be made to terminology (e.g., “defend step” and “defender action” instead of “block step” and “block action”), which are discussed in **Sec. 3**. While defect check developers can use the IR 8011 methodology with other control-based frameworks, the IR 8011 series will continue to identify defect checks based on controls in SP 800-53 [7] and procedures in SP 800-53A [9].

## 3. Updated Guidance and Updated Language

Volume 1 will be restructured before new volumes are developed and existing volumes updated. All new volumes and all revised (existing) volumes will follow the new Volume 1 structure. IR 8011v1 will also be updated to include multiple notional implementation and use examples, some of which are previewed in **Appendix A**. New guidance will also be provided for each item in **Sec. 2**.

The language used in the IR 8011 Series will also be updated. The new title for the IR 8011 Series will be *Automation Support for Control Assessments*. The term "security" will be removed to reflect how the Series supports any control, not just security controls. This aligns with other RMF-supporting publications that reference "controls" and "control assessments" rather than "security controls," "privacy controls," "security control assessments," or "privacy control assessments."

The terms "block step" and "block action" will be replaced with "defend step" and "defender action." IR 8011 indicates that blocking or delaying an attack is a response to an attack. However, "blocking" is just one way to defend, and a defense may not be in the form of blocking. Therefore, the "attack step" and "defend step" pairing is more appropriate.

Moreover, biased terminology has been deprecated and replaced with more specific and inclusive terms. For example, the terms "whitelist" and "blacklist" will be replaced by "allowlist" and "denylist."

Finally, all volumes will be revised to use plain language, which facilitates readability and translations of the material.

## 4. Interested Party Engagement

The IR 8011 Team would like to expand collaboration beyond the traditional draft publication comment process in which draft versions are released for public comment and comments are reviewed, analyzed, and acted upon (if necessary) before a final version is published. Increasing the involvement of interested parties will improve the quality of these publications and promote collaboration to assist in the operationalization of IR 8011.[14]

### 4.1. Interested Party Identification

Interested parties are individuals and organizations that:

- Can help operationalize[15] IR 8011.
- Can provide feedback to the IR 8011 Team on the contents of the Series' volumes.
- Use/adopt or may be interested in using/adopting an IR 8011 solution.
- Have an academic interest in the methodology.

In February 2023, the IR 8011 Team issued a call for adoption feedback "to better understand the use of the IR 8011 series by adopters, success stories, what adopters liked/disliked about the methodology and about the series overall, the challenges (if any) adopters faced during implementation, and how we can improve the entire series" [9]. In response, a few individuals and organizations shared their experience with IR 8011 and indicated interest in collaborating on the development and maintenance of the IR 8011 Series. That was the first step in the identification of potential interested parties. The IR 8011 Team will continue to identify interested parties through outreach activities.

### 4.2. Community of Interest (CoI)

To facilitate collaboration, the IR 8011 Team proposes the establishment of a Community of Interest (CoI) in which developers, current and future adopters, and other enthusiasts can work together to identify action items, propose solutions to problems, and discover opportunities for improvement.

Individuals and organizations who work or are planning to work with IR 8011 and who are interested in joining the IR 8011 CoI can contact the IR 8011 Team at 8011comments@list.nist.gov.

### 4.3. IR 8011 Portal — Companion Website

To better support the IR 8011 community, the IR 8011 Team will dedicate a portion of the NIST RMF Project website [10] to host information and resources, such as learning materials (e.g., IR 8011 Quick Start Guides), CoI membership and activity information, news and announcements, vendor and innovator showcasing, and other highlights.

[14] See **Sec. 5** for a discussion on the operationalization of IR 8011.
[15] *Ibid.*

## 5. Operationalization of IR 8011

In simple terms, IR 8011 will be operationalized by a solution developer or provider who can use the technical specifications and guidance in each volume to develop a commercial or non-commercial solution that an adopter can use.[16]

The proposed update to the IR 8011 methodology can give solution providers the autonomy to apply the (updated) methodology to create any defect check. This flexibility can enable developers and vendors of governance, risk, and compliance (GRC) tools to integrate IR 8011 into their products.

The ultimate goal of the project is the operationalization of IR 8011 to ensure that the NIST-produced "blueprint" for supporting the assessment of controls is transformed into a solution that can benefit agencies and organizations.

[16] Note that the NIST RMF Team does not develop implementation solutions for its technical publications.

## 6. IR 8011 Project and Development Roadmap

The following project activities are planned:[17]

- Publications
    - IR 8011, Volumes 1 through 4, Revision 1 release
    - IR 8011, Volumes 5 through 9 release
- Resources
    - IR 8011 portal (companion website) launch
    - IR 8011 CoI launch
    - IR 8011 CoI mailing list launch
    - IR 8011 Quick Start Guides release

The IR 8011 Team will address the findings captured in this report as expeditiously as possible. However, the prioritization of efforts may be affected by new government initiatives and resource availability that supersede planned IR 8011 development and maintenance. The maintenance of published volumes includes revisions that account for major updates to SP 800-53 [7] and SP 800-53A [9].

[17] Subject to change without notice.

## 7. Conclusion

There is so much potential for making control assessments more accurate and more efficient. Once solutions are built, offered, and adopted, control assessments can be expedited and produce more accurate results through automation. While NIST is designing and offering a blueprint to support the automation of control assessments, it is the community — the innovators — who will turn that blueprint into a reality.

Testing controls and control items is just one fraction of the control assessment process described in SP 800-53A [9]. Interviews and examinations are still widely used to evaluate the implementation, completeness, and effectiveness of controls. Often, these other assessment methods[18] (i.e., interviews and examinations) are necessary to complement control testing to fully assess a single control. Nonetheless, control testing can enable automated assessments, which, in turn, can support ongoing assessments, ongoing authorizations, and continuous monitoring.

The NIST is committed to making the operationalization of IR 8011 possible by improving its guidance and technical specifications, as well as engaging with the community to promote effective collaboration. NIST believes that this collaborative work will lead to improved products and guidance and, ultimately, an implementable IR 8011 solution.

[18] For more on assessment methods, see **Sec. 2.4.2** of SP 800-53A [9]

## References

[1] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[2] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 1. https://doi.org/10.6028/NIST.IR.8011-1

[3] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 2. https://doi.org/10.6028/NIST.IR.8011-2

[4] Dempsey KL, Goren N, Eavy P, Moore G (2018) Automation Support for Security Control Assessments: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 3. https://doi.org/10.6028/NIST.IR.8011-3

[5] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[6] Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 4. https://doi.org/10.6028/NIST.IR.8011-4

[7] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[8] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[9] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[10] National Institute of Standards and Technology (2023), *Call for Feedback: NIST IR 8011 Series Adoption*. Available at https://csrc.nist.gov/news/2023/call-for-feedback-nist-ir-8011-series-adoption

[11] National Institute of Standards and Technology (2023), *NIST Risk Management Framework (RMF) Project*. Available at https://nist.gov/rmf

[12] National Institute of Standards and Technology (2023), *NIST Cybersecurity and Privacy Reference Tool (CPRT).* Available at https://csrc.nist.gov/projects/cprt

## Appendix A. Notional Implementations and Uses for IR 8011

This appendix provides examples of potential ways to adopt IR 8011. The examples are intended to provide context for the application and use of the IR 8011 methodology. Developers, solution providers, and adopters are encouraged to apply and use the IR 8011 methodology in innovative and secure ways. They are also encouraged to share their implementation with the IR 8011 Team (via 8011comments@list.nist.gov) and the broad community through the planned Community of Interest.

### A.1. Integration of IR 8011 Defect Checks Into GRC and ISCM Solutions

An effective GRC tool can help manage security and privacy risks by supporting the implementation and monitoring of certain controls. GRC applications often provide a central repository of security-relevant data, including desired and actual state data so they can be excellent candidates for defect check integration.

Whether the integrated defect checks are organized by ISCM security capability or not, authorized users of the GRC application could manually run defect checks or schedule them to be automatically executed according to a predefined schedule. Depending on the user's role (i.e., the individual or service executing the defect check) and application use, the automated assessment can support self-assessment activities, external or independent assessment activities, and internal monitoring activities. Thus, a continuous monitoring solution may also be equipped with the ability to automatically assess controls through the implementation of the IR 8011 methodology.

### A.2. Support for Internal Automated Control Assessments

Tests can be individual scripts that are bundled to assess controls on a control-by-control basis, control family basis, or on an ISCM security capability basis. These scripts can be supported by a simple supporting configuration (i.e., "setup") as long as desired and acceptable state specification data exist and actual state data can be collected. The setup does not need to be a complex security architecture. In fact, the data collection, analysis, and reporting processes may or may not be fully automated.

This particular notional implementation may be an attractive option for leveraging IR 8011 for internal (self-) assessments.

Practical example:

- Defect Check HWAM-F01, *Unauthorized devices*
    - (*Sample*) **Desired state:** Inventory list of the MAC addresses of all authorized devices that can be admitted to the network
    - (*Sample*) **Actual state:** MAC addresses of all devices on the network
    - (*Sample*) **Response:** Remove device

- (*Sample*) **Implementation:** To collect actual state data, software-based network sensors are placed within the network boundary to detect all devices on the network. Detection of the devices requires the identification of all of the devices already present on the network (wired or wireless) as well as any new devices that join the network. A simple check involves comparing the MAC addresses of the devices on the network to an existing list of approved MAC addresses. If there is no match (i.e., if a detected MAC address is not listed on the approved list), then automatically remove the device by blocking or rejecting the MAC or IP address of the unauthorized device. The comparison can be scripted (e.g., using regular expressions), and the device can be blocked automatically via network utility software.[19]

Although the simplicity of developing internal tools can be attractive to an organization, there must be rigor in the development and maintenance of the scripts and supporting information technology infrastructure. This includes design, testing, configuration management, maintenance, and other concerns.

### A.3. Support for External Independent Automated Control Assessments

External independent automated control assessments may leverage a combination of the two notional implementation and use examples in A.1 and A.2. The intent is to take advantage of any on-premises implementation at the customer's site (i.e., site of the system or organization being assessed) and any operational tests utilized by the external independent assessor or assessment team.

There are challenges to allowing external independent assessors to run automated control assessments utilizing internal repositories of desired state data maintained at the customer's site, such as access control, permissions, and integration difficulties that are inherent to connecting an external resource to an internal resource. Most importantly, such integration may incur risks to the organization. Therefore, the security of the system architecture is reviewed and analyzed before allowing an external entity to access an internal network and resources.

In its most simplistic approach, the external independent assessor would only require access to the on-premises implementation at the customer's site and would use the customer's existing resources (e.g., the customer's GRC tool/repository with or without an integrated IR 8011 functionality, such as support for running defect checks) to validate and verify the assessment and assessment results. A more complex implementation would require the external independent assessor to run their own implementation of IR 8011, which may include the use of their own data repositories for (customer) desired state and actual state information, as well as their own implementation of and mechanisms for actual state collection and state analysis.

[19] This is only an illustrative implementation for educational purposes. There may be drawbacks to relying on actual data that can be spoofed (e.g., MAC addresses).

### A.4. Automated Control Assessments as a Service

Setting up and integrating the infrastructure to support automated control assessments and continuous monitoring presents additional challenges, such as architectural changes and allowing an external independent assessor or team to conduct automated assessments within the organization's boundary. A potential solution may be a cloud-based infrastructure that features an ISCM collection system with a direct and secure link to the assessment boundary. Automated control assessments as a service may also address some of the challenges involved in establishing an on-premises infrastructure.

### A.5. Keyword Searches

Electronic keyword searches are important for the development of defect checks and must produce accurate results with minimal to no false positives or false negatives. Manually (i.e., visually) searching controls by keyword is time-consuming and may not yield accurate results. Searching the entire control catalog in portable document format (PDF) would also include the front matter and all text up to Sec. 2 of SP 800-53 [7]. Therefore, consider using control data sets instead of actual publications for the keyword searches.

When using IR 8011 to support the automation of SP 800-53 [7] control assessments, adopters can take advantage of the various data formats of the SP 800-53 [7] control catalog that are offered free of charge via the NIST Cybersecurity and Privacy Reference Tool (CPRT)[20] [11]. The raw data can be put into a database or spreadsheet to facilitate keyword searches. Make sure that the Discussion text remains in scope for the searches since there are more keywords in the Discussion text than in the control name and description fields.

[20] As of the time of this writing, the CPRT search function only allows for exact matches.