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.

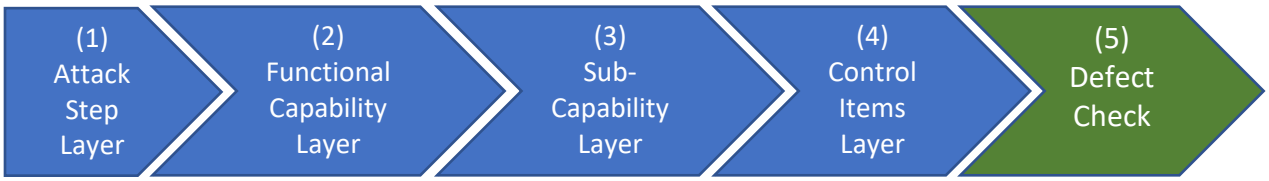

Fig. 1. IR 8011 methodology workflow summarized as security capability abstraction layers

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.

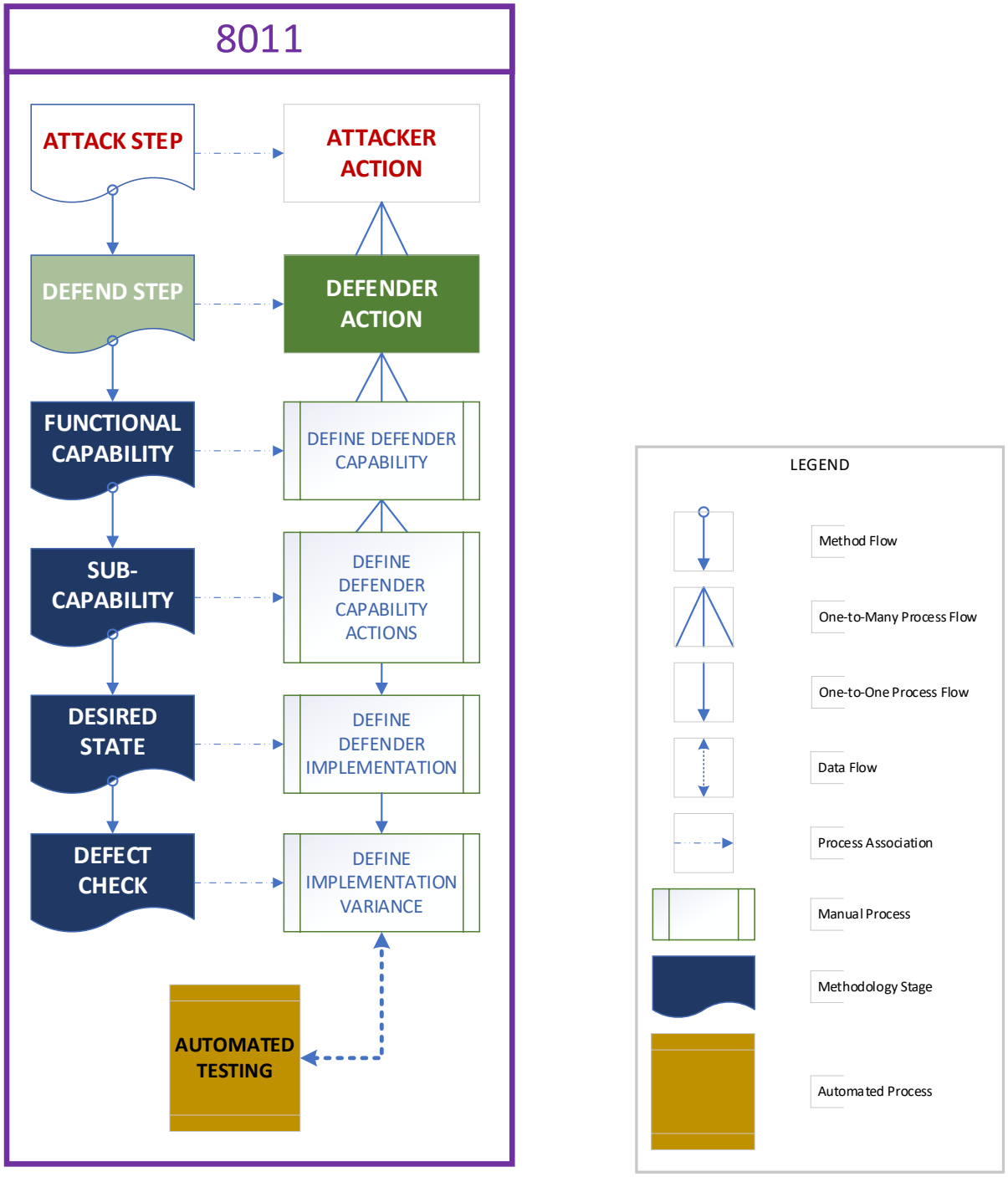

Fig. 2. Updated IR 8011 methodology workflow with output