Draft NIST Special Publication 800-137A

Assessing Information Security Continuous Monitoring (ISCM) Programs:

Developing an ISCM Program Assessment

Kelley Dempsey
Victoria Yan Pillitteri
Chad Baer
Robert Niemeyer
Ron Rudman
Susan Urban

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-137A-draft

INFORMATION SECURITY

Sponsored by U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Draft NIST Special Publication 800-137A

Assessing Information Security Continuous Monitoring (ISCM) Programs:

Developing an ISCM Program Assessment

Kelley Dempsey
Victoria Yan Pillitteri
Computer Security Division
Information Technology Laboratory

Chad Baer
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Robert Niemeyer
Ron Rudman
Susan Urban
The MITRE Corporation
McLean, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-137A-draft

January 2020

Cybersecurity and Infrastructure Security Agency
Christopher C. Krebs, Director

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

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-137A
Natl. Inst. Stand. Technol. Spec. Publ. 800-137A, 78 pages (January 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-137A-draft

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 cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *January 13, 2020* through *February 28, 2020*

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 information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication describes an approach for the development of Information Security Continuous Monitoring (ISCM) program assessments that can be used to evaluate ISCM programs within federal, state, and local governmental organizations, and commercial enterprises. An ISCM program assessment provides organizational leadership with information on the effectiveness and completeness of the organization's ISCM program, to include review of ISCM strategies, policies, procedures, operations, and analysis of continuous monitoring data. The ISCM assessment approach can be used as presented or as the starting point for an organization specific methodology. It includes example evaluation criteria and assessment procedures that can be applied to organizations.

Keywords

assessment; assessment element; assessment methodology; assessment procedure; continuous monitoring; information security continuous monitoring; ISCM program; ISCM program assessment.

Acknowledgments

The authors wish to thank Mr. Jeff Finke and Mr. Tracy Teter of The MITRE Corporation for their detailed reviews of this publication. The authors also wish to thank the numerous reviewers for their insightful feedback. The authors also gratefully acknowledge the contribution of the Cybersecurity Assurance Branch at the Cybersecurity and Infrastructure Security Agency whose members piloted the initial version of the ISCM methodology on which this publication is based, and wish to thank the Cybersecurity Division of CISA for sponsoring the development of this publication. In addition to the above acknowledgments, a special note of thanks goes to Jim Foti, Lorin Smith and the NIST web team for their outstanding administrative support.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sec-cert@nist.gov

Executive Summary

To effectively manage cybersecurity risks, organizations require ongoing awareness of their information security posture, vulnerabilities, and threats.[1] Organizations face the continual challenge of providing timely and complete security information with which to make risk-based management decisions. To achieve awareness and better manage risks, organizations implement Information Security Continuous Monitoring (ISCM) capabilities under direction of an ISCM program. An ISCM program defines, establishes, implements, and operates the various aspects of ISCM to provide the organization with the information necessary to make risk-based decisions regarding security status at all organizational risk management levels.

Organizations need a way to determine and evaluate if an established ISCM program is effectively managing the organization's security posture, commensurate with risk. This publication describes one approach to developing an ISCM program assessment based on evaluation criteria derived from multiple sources, e.g., NIST Special Publications (SP) 800-137, SP 800-37, SP 800-39, and Office of Management and Budget (OMB) Circulars and Memoranda. An ISCM program assessment developed under guidance in this publication evaluates the ISCM program itself and not the results of the ISCM program or the technologies used. An effective ISCM program assessment provides consistent results and is independent of those conducting the ISCM program assessment.

An ISCM program assessment provides a means for evaluating an organization's ISCM strategies, policies, procedures, implementations, operational procedures, analytical processes, specific reporting and ISCM results presentation, risk assessment and risk scoring, risk response, and the ISCM program improvement process. An ISCM program assessment may be developed by an organization to evaluate its own ISCM program or by an organization that assesses other organizations.

Creating or adopting and using an ISCM program assessment can help reduce overall risk to organizations by identifying gaps in an ISCM program, in the implementation, or in the operational use of ISCM results. In addition, an ISCM program assessment can indicate the level of readiness for system-level ongoing authorization.
This publication:

- Offers guidance on the development of an ISCM program assessment process for all organizational risk management levels (organization level, mission and business process level, and system level), as defined in NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective;*

- Describes how an ISCM program assessment relates to important security concepts and processes, such as the NIST Risk Management Framework (RMF), organization-wide risk management levels, organizational governance, metrics applicable to ISCM, and ongoing authorization;

[1] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* defines ISCM as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions" [SP800-137, p. B-6]

- Describes the properties of an effective ISCM program assessment;
- Presents a set of ISCM program assessment criteria, with references to the sources from which the criteria are derived, that can be adopted by an organization and used for ISCM program assessments or as a starting point for further development of an organization's assessment criteria; and
- Defines a way to conduct ISCM program assessments by using assessment procedures, defined in the companion document containing the ISCM Program Assessment Element Catalog, designed to produce a repeatable assessment process.

Table of Contents

List of Figures

List of Tables

1 Introduction

Federal agencies, under the Federal Information Modernization Act of 2014 (FISMA) [FISMA2014] and Office of Management and Budget (OMB) circulars and memoranda,[2] are directed to implement a program to continuously monitor organizational information security status. A comprehensive continuous monitoring program serves as a risk management and decision support tool used at each level of an organization. Strategies and business objectives at the organizational level direct activities needed at the mission and business level and direct system level functions and technologies implemented in support of continuous monitoring.

NIST Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [SP800-137] defines information security continuous monitoring (ISCM) as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An ISCM program defines, establishes, implements, and operates the various aspects of ISCM to provide the organization with the information necessary to make risk-based decisions regarding security status at all three organizational risk management levels.

To effectively address increasing security challenges, the ISCM program:

- Addresses assessment of security controls for effectiveness and security status monitoring;[3]
- Promotes the concept of near real-time risk management and ongoing system authorization through the implementation of robust organization-wide continuous monitoring processes; and
- Incorporates processes to ensure response actions are taken in accordance with findings and organizational risk tolerances, and to ensure response actions have the intended effects.

This publication provides guidance on how an organization can assess ISCM program completeness and effectiveness and detect deficiencies in its ISCM program. The goal of the ISCM program assessment is to provide a means for evaluating organizational ISCM program elements, including the review of ISCM strategies, policies, procedures, implementation planning, ISCM metrics, analytical processes, specific results presentation and reporting, risk scoring, risk response, and the ISCM improvement process. The approach used throughout this publication is based on the concepts and principles of [SP800-137] and the ISCM requirements mandated for federal organizations.

The term *assessment* is used in two ways in this publication. *Assessment* may refer to the completed action of ISCM program evaluation or to the vehicle that is reused for each evaluation

[2] OMB Circular A-130 (2016) [OMB A-130], OMB Memoranda M-14-03 [OMB M-14-03], and M-11-33 [OMB M-11-33] are the primary directives. OMB M-14-03 requires all federal agencies to establish an ISCM program in accordance with NIST SP 800-137. OMB M-11-33 requires that the ISCM program be periodically reviewed to ensure that continuous monitoring is adequate for supporting risk-based decisions. OMB Circular A-130 reiterates and formalizes the Memoranda requirements.

[3] Security status monitoring is the monitoring of organizationally defined metrics that measure the organizational security posture.

(e.g., a template or blank worksheet). The context in which the term is used conveys the applicable meaning.

1.1 Background

Organizations face the continual challenge of providing timely and complete security information with which to make risk-based management decisions, which is the objective of the ISCM program. An effective ISCM program produces timely security-related information that is accurate and complete for presentation to decision makers at multiple levels of the organization. At the organizational level, it may not be well understood how, where, and why the ISCM program fits into the organization-wide risk management strategy. It is crucial for the organization's leadership to understand how business needs and capabilities drive the ISCM program. In many cases, capabilities needed for organizational continuous monitoring may already exist within the organization. However, without a comprehensive strategy to formally codify monitoring capabilities as enabling ISCM functions, a true ISCM program does not exist.

Organizations need a method of evaluating what has been planned, developed or acquired to implement ISCM, particularly if the ISCM program was developed internally. This helps determine whether the organization's ISCM program is adequate and the money spent is providing value.

To determine the effectiveness of an organization's ISCM program, the organization develops and uses a formal assessment for evaluating the program that provides organizational leadership with information about how well the ISCM program meets its intended objectives. An ISCM program assessment may comprise evaluation criteria, judgments, and scores about specific aspects of ISCM capabilities, and conclusions based on the analysis of collected data. An ISCM program assessment may also provide recommendations to the organization based on assessment results.

Under sponsorship of the Cybersecurity and Infrastructure Security Agency (CISA),[4] in conjunction with the National Cybersecurity Center of Excellence (NCCoE) at NIST, initiated development of an ISCM program assessment process based primarily on [SP800-137], published by the NIST Computer Security Division (CSD).

The assessment process, which is presented in more detail in the forthcoming NIST Interagency or Internal Report (NISTIR) 8212 [NISTIR8212], was developed for use by CISA and federal agencies. The ISCM program assessment process can be tailored for use by federal agencies, commercial organizations, and non-federal governmental organizations. Using this publication as a guide, an organization may choose to adopt the same approach to evaluating ISCM plans and solutions.

1.2 Purpose

This publication:

- Provides guidance on the development of an ISCM program assessment for all organizational risk management levels;
- Defines a methodology to conduct ISCM program assessments;
- Presents a set of detailed ISCM program assessment criteria that can be adopted by an organization or assessing organization; and
- Describes the properties of an effective ISCM program assessment.

In addition, the guidance presented in this publication can be used to produce an ISCM program assessment to:

- Evaluate planned modifications to an existing ISCM program;
- Guide the direction of a planned or future ISCM program by providing a starting point for ISCM development; and
- Ensure the inclusion of monitoring the effectiveness of specifically recognized national or organizational priority items; such as insider threats, or high priority/visibility initiatives (e.g., high value assets) in the ISCM program assessment.

1.3 Audience

This publication serves individuals associated with the continuous monitoring of information security posture and organizational risk management, including:

- Individuals responsible for the review of an organization's ISCM program, to include management and assessors who conduct technical reviews, e.g., system evaluators, internal and third-party assessors/assessment teams, independent verification and validation assessors, auditors, and system owners;

[4] For more information about CISA, see: https://www.cisa.gov.

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities, e.g., heads of federal agencies, chief executive officers, and chief financial officers;
- Individuals with system development and integration responsibilities that consider ISCM functionality, e.g., program managers, system owners, information technology product developers, system developers, systems integrators, enterprise architects, information security architects, and common control providers;
- Individuals with system and/or security management/oversight responsibilities, e.g., senior leaders, risk executives, authorizing officials, chief information officers, chief information security officers[5], who make risk-based decisions based, in part, on security-related information generated from continuous monitoring; and
- Individuals with system and security control assessment and monitoring responsibilities, e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, system owners, or system security officers.

1.4 Scope

This publication addresses the entire ISCM program assessment process and is used to evaluate the establishment and operation of ISCM programs across organizations.

There are many ways to evaluate an organizational program or system against a set of criteria. This publication specifies one approach to developing assessments for doing so based on evaluation criteria derived from multiple sources. The ISCM program assessment evaluates the structure and governance of the ISCM program and does not evaluate the continuous monitoring technologies or implementations themselves. An assessment developed under the guidance provided herein is technology-neutral, flexible, and scalable to be easily adopted by any organization and applied to any type of security monitoring technology. Organizations are encouraged to use the approach specified in this publication as a starting point to develop an assessment to better meet specific organizational needs.

1.5 Assumptions

It is assumed that the reader is familiar with the ISCM concepts described in [SP800-137] and has a working-level understanding of the NIST Risk Management Framework (RMF) as defined in [SP800-37], as amended. It is also assumed that the reader is familiar with risk management processes across the organization and organizational levels as defined in NIST SP 800-39 [SP800-39], *Managing Information Security Risk: Organization, Mission, and Information System View*, as amended.

1.6 Organization of this Publication

The remainder of this NIST Special Publication is organized as follows:

[5] At the *federal* organizational level, this position may be known as the Senior Agency Information Security Officer (SAISO). Organizations may also refer to this position as the Senior Information Security Officer (SISO) or the Chief Information Security Officer (CISO).

- Section 2 describes the fundamentals of assessing an organization's ongoing monitoring of information security (i.e., ISCM) in support of risk management, ISCM background, interaction with NIST RMF, ISCM program assessment criteria and their sources, ISCM program assessment criteria development, and using the ISCM program assessment. Topics described in Sec. 2 are somewhat independent of each other.
- Section 3 describes the process of assessing ISCM programs, including planning and execution of assessments, assessment procedures, and the use of results. Section 3 presents an integrated assessment process using the topics introduced in Sec. 2.
- A References section lists general references found in this publication.
- Supporting appendices provide additional information regarding ISCM including: (A) acronyms; (B) glossary; and (C) diagrams showing relationships among the assessment elements.
- A separate spreadsheet provides a complete catalog of the assessment elements and assessment procedures that can be used to build an ISCM program assessment [Catalog].

2 The Fundamentals

This section explains the fundamentals of the ISCM program assessment, a management process that provides a view into the adequacy and effectiveness of the:

- ISCM strategy and planning;
- Establishment of the ISCM program;
- Implementation of ISCM strategies, policies, and metrics;
- Operation of the ISCM program;
- Analysis of data collected and reporting of results;
- Response to ISCM results; and
- ISCM process improvement.

The fundamentals presented in this section are integrated into an assessment process in Sec. 3.

The development process of the ISCM program assessment does not seek to evaluate the organization, its missions/business processes, and systems for every ISCM concept presented in [SP800-137]. The ISCM program assessment determines if the concepts, along with ISCM requirements levied on federal organizations by FISMA and OMB, are sufficiently addressed[6] to permit a determination of ISCM program robustness.[7] It should be noted that each organization or assessor developing an ISCM program assessment from the guidance in this publication is likely to produce different assessment criteria depending on what is important to the organization or assessor.

2.1 ISCM Management

ISCM is an organization-wide responsibility first, then a system-level responsibility [SP800-37], to include mission and business processes as well. Organization-wide continuous monitoring efforts begin with organizational leadership defining a comprehensive, organization-wide ISCM strategy that directly supports decision making within the risk executive function and includes consistently managed metrics linked to each organizational risk management level.[8] Only when an ISCM strategy is defined and adopted at the organizational level, and intrinsically linked to the risk executive function, can the ISCM program be established with the appropriate breadth and depth to provide all levels of the organization with clearly defined responsibilities. The organizational level strategy is supported by system-level ISCM strategies and, optionally, mission/business process ISCM strategies.

[6] This approach has been validated through early organizational assessments of federal government departments and agencies conducted by CISA.

[7] When applied to ISCM programs, "robustness" refers to an ISCM capability that is sufficiently accurate, complete, timely, and reliable to provide security status information to organization decision-makers to enable them to make risk-based decisions.

[8] [SP800-39] identifies the organizational risk management levels – organization level (level 1); mission/business process level (level 2); and system level (level 3).

ISCM encompasses all the people, policies, processes, technologies, and standards that are used to perform the continuous monitoring function. ISCM is an enabling process that supports or provides organizational sustainment in the face of cybersecurity threats and risks.

An adequately-developed ISCM program identifies the specific activities at each level of the organization that enable an organization-wide ISCM function. To effectively support the overall ISCM effort, ISCM activities are consistently developed, deployed, and sustained with explicit mapping to the ISCM strategic objectives and risk management strategy for the entire organization.

The following subsections summarize important ISCM concepts and introduce how the ISCM program assessment relates to each concept. For additional details of ISCM, see [SP800-137].

2.1.1 ISCM Background

ISCM goals include detection of anomalies and changes in the organization's environments of operation and systems, visibility into assets, awareness of vulnerabilities and threats, and knowledge of security control effectiveness, and security posture. To meet ISCM goals, tools, technologies, and manual and automated methods are implemented within the context of an ISCM architecture designed to deliver the required information in the appropriate context, at the right level of detail, and at the right frequencies. The key outcome of the ISCM program is to enable the collection, integration, analysis, and presentation of security-related information from all systems and their environments of operation across the organization to inform risk-based decision making.[9]

An effective ISCM program identifies manual and automated monitoring processes in the organization-wide ISCM strategy, integrates the processes and associated outputs, and incorporates results into a view of situational awareness. Where manual processes are used, the processes are verified so that they are repeatable and enable a consistent implementation. Automated processes, including the use of automated support tools, can make the process of continuous monitoring more consistent, efficient, and cost-effective.

An effective ISCM program facilitates ongoing authorization and reauthorization decisions for systems [SP800-37], as discussed in Sec. 2.1.7. Security-related information collected during continuous monitoring is used to make updates to the authorization package and supporting artifacts for each applicable system. Updated artifacts provide evidence that the baseline security controls continue to safeguard the system as originally planned.

2.1.2 ISCM Process Steps

NIST SP 800-137 organizes the ISCM process into six steps, as depicted in Figure 1 and explained below. It is important to note that any effort or process intended to support ongoing monitoring of information security across an organization begins with the development of a

[9] For federal agencies, a uniform approach to ISCM across the federal government allows OMB and DHS to assess the security posture of the federal government as a whole. The same rationale applies to nonfederal organizations.

comprehensive ISCM strategy - encompassing technologies, processes, procedures, operating environments, and people.

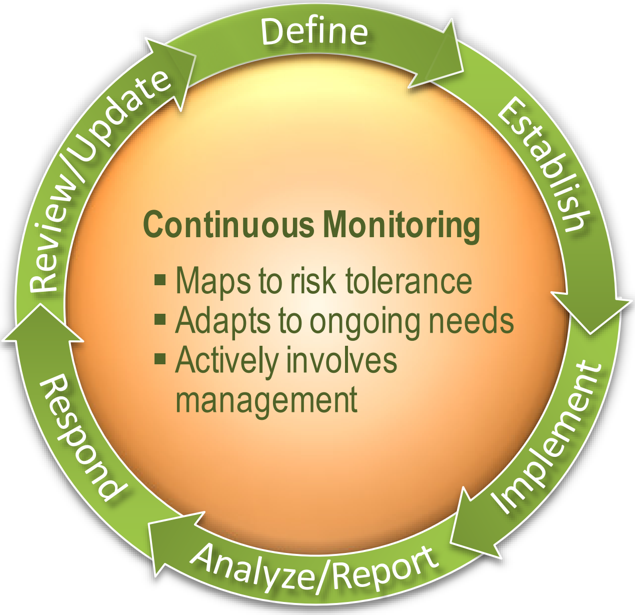


Figure 1 – ISCM Process.

The six ISCM steps are referred to as "process steps" in this publication, and are:

1. **Define ISCM Strategy (Define)** – Define the organization-wide and system-level ISCM strategies based on organizational risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts. A system-level ISCM strategy consistent with the organization-wide ISCM strategy is defined for each system within the organization. A mission/business process area may also define an ISCM strategy that is consistent with the organization-wide strategy and applies to the systems supporting the mission/business process area.

2. **Establish ISCM Program (Establish)** – Establish an ISCM program, determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.

3. **Implement ISCM Program (Implement)** – Implement the ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.

4. **Analyze ISCM Data and Report Findings (Analyze/Report)**– Analyze the data collected, report findings, and determine the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

5. **Respond to ISCM Findings (Respond)** – Respond to findings with technical, management, and operational risk mitigating activities, or accept, transfer/share, or avoid/reject the risk.

6. **Review and Update ISCM Program and Strategy (Review/Update)** – Review and update the monitoring program, adjusting the ISCM strategy at the applicable level, and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

The organization-wide, the system-level, and the optional mission/business process ISCM strategies are defined in the ISCM Define step. The organization-wide and the optional mission/business process ISCM strategies are addressed in the RMF Prepare step for Level 1and Level 2, and the system-level ISCM strategy is addressed in the RMF Select Step for Level 3 (see [SP800-37]).[10]

2.1.3 Organization-wide Risk Management Levels

ISCM applies to all three organizational risk management levels[11] defined in [SP800-39], which are:

- **Level 1** (organization level) addresses risk across the *entire organization* and informs Levels 2 and 3 of risk context and risk decisions made at Level 1;
- **Level 2** (mission or business process level) addresses risk from a mission/business process perspective and is informed by risk context, risk decisions, and risk activities at Level 1; and
- **Level 3** (system level) is the system-oriented level within the organization; Level 3 focuses on system activity and is guided by the risk context, decisions, and activities at Level 1 and Level 2.

Security-related information is obtained and acted on at Level 3 and is communicated to Levels 1 and 2 to be incorporated in organization-wide and mission/business process risk determinations. The ISCM program assessment verifies the flow of information between levels.

2.1.4 NIST Risk Management Framework and ISCM

The RMF, defined by [SP800-37], is a disciplined and structured process that integrates information security and risk management activities into the system development life cycle for organizations and systems. Implementation of the ISCM program may rely on artifacts and

[10] The term "Level" is adapted from NIST [SP800-39].
Level 1 addresses risk from an *organizational perspective* by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions. In this publication, Level 1 pertains to the personnel responsible for the overall risk strategy, policies, and procedures of the entire organization.
Level 2 addresses risk from a *mission/business process* perspective by designing, developing, and implementing mission/business processes that support the missions/business functions defined at Level 1. In this publication, Level 2 pertains to the personnel responsible for the mission or business process ISCM strategy, policies, and procedures of a sub-organization related to a specific mission or business process (but not the entire organization).
The risk management activities at Tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission/business functions of organizations. In this publication, Level 3 pertains to the personnel responsible for implementing ISCM for specific systems.

[11] NIST SP 800-37 Revision 2 renames *tiers* to *levels*. In a forthcoming update to NIST SP 800-39, the term *tiers* will also be updated to *levels*.

processes implemented as part of the RMF and also provides input to the RMF steps to understand and manage risk; the assessment approach and assessment elements address any potential overlap and/or relationships.

The RMF *Monitor* step describes continuous monitoring, which is a critical part of the risk management process. ISCM can meet requirements of organizational continuous monitoring and provide results that can be used in the identification of and response to risk. In addition, an organization's overall security architecture and accompanying security program are monitored through ISCM to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that occur. Timely, relevant, and accurate security-related information is vital, particularly when resources are limited, and organizations must prioritize their efforts.

At Level 3, the RMF *Monitor* step and ISCM activities are closely aligned. The assessment methods relevant for implemented controls are the same, whether the assessments are performed solely in support of system authorization (the RMF *Authorize* step) or in support of a broader, more comprehensive continuous monitoring effort. System-level officials and staff conduct assessments and monitoring, analyzing results on an ongoing basis. The information obtained is leveraged at the organization, mission/business processes, and system levels to support risk management.

Although frequency requirements may differ, each organizational level receives the benefit of security-related information that is current and applicable to affected processes. RMF *Monitor* activities that are performed within the context of the ISCM program and support system risk determination on an ongoing basis are foundational for ongoing authorization (OA). When the ISCM program is found to be adequate for determining risk across all (or part) of the organization, ISCM supports OA across all (or part) of the organization. The ISCM program assessment verifies that applicable ISCM results, which may include relevant metrics, are made available to the OA process to make the decisions about system authorization. OA is discussed in Sec. 2.1.7.

2.1.5 Governance and ISCM

ISCM governance is part of overall organizational governance, which provides oversight to organizations by specifying authorities, responsibilities, accountability, and governing processes and procedures that facilitate implementation, enforcement, and continuous improvement of the ISCM governing processes. Governance, including ISCM governance, establishes lines of accountability throughout the organization at all risk-management levels.

ISCM governance is a conceptual organizing and planning structure for managing risk. It is linked to one or more senior officials or staff, such as the risk executive (function) or other accountable senior official, e.g., senior accountable official for risk management, senior agency information security officer (SAISO), senior agency official for privacy, and chief information officer (CIO). The part of information security governance structure addressing ISCM is aligned with other governance structures to ensure compatibility with established management practices within the organization and to increase overall effectiveness.

The ISCM program assessment verifies that ISCM governance policies and processes exist and are being followed. At Level 1, an assessment verifies that senior leaders recognize the importance of managing information security risk and establish appropriate governance structures relative to ISCM for managing such risk. The organization-wide ISCM strategy captures the ISCM governance structures.

Where the organization has decentralized governance (e.g., because of divergent mission or business needs or operating environments), mission/business process areas, while remaining consistent with the organization-wide ISCM strategy, may establish their own ISCM policies and processes, in whole or in part, particularly as they relate to risk management and information security decisions. With the decentralized governance model, it is important that the different levels of the organization share ISCM information as it relates to risk management decisions.

2.1.6 ISCM Metrics

Metrics determined through ISCM provide important information about the security posture across the organization and relative to individual systems and inform the risk management process. See [SP800-137] for details on ISCM metrics.

The ISCM program assessment does not dictate specific metrics to be evaluated, but rather accommodates organization-defined metrics. The ISCM program assessment verifies that the ISCM program addresses the specification, development, maintaining, and sustaining of metrics. The ISCM program assessment also verifies that the organization: (i) specifies frequencies of collecting metrics data; (ii) determines metrics from data at Levels 1, 2, and 3; and (iii) applies the metrics as needed to make risk-based decisions. In addition, the ISCM program assessment verifies that ISCM metrics are reported to designated officials at each level who review the relevant metrics.

2.1.7 Ongoing Authorization

ISCM benefits the organization by facilitating OA, which streamlines the system authorization process and supports a more automated ability to make near real-time risk-based decisions on whether to continue system authorization. OA is defined as the subsequent (follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. OA is fundamentally related to the ongoing understanding and ongoing acceptance of security risk and is dependent on a robust ISCM program.

Organizations make OA decisions for systems by leveraging security-related information gathered through the ISCM capability. A robust ISCM program defines, establishes, and implements a continuous process by which manual, automated, and procedural tools can be used to manage and govern the risks of operating authorized systems.

The ISCM program assessment verifies that ISCM information is made available for making OA decisions. The ISCM program assessment verifies that:

- There is an organization-wide process for OA. The OA process addresses how systems transition into OA status and conditions necessary for a system to remain in OA status;

- Control assessments (in accordance with NIST SP 800-53A) are conducted at a documented frequency sufficient to support OA;
- The metrics provided by the ISCM program are considered sufficiently stable and robust for informing OA decisions;
- The ISCM program monitors the security status of systems and the environments in which those systems operate on an ongoing basis with a frequency sufficient to make ongoing, risk-based decisions on whether to continue to operate the systems within the organization; and
- ISCM results are reported to appropriate officials who make ongoing authorization decisions.

2.2 Foundation of ISCM Program Assessments

The goal of an ISCM program assessment is to provide an organization with actionable recommendations to improve the ISCM program. ISCM program assessment results include an indication of how well the assessed organization (entire organization, mission/business process, or system) meets the evaluation criteria. Assessment results give indications of ISCM program adequacy and consistency. Results may also include recommendations for ISCM program design, implementation, operation, and governance that may need improvement.

The ISCM program assessment process is an information-gathering and evidence-analyzing activity. The information gathered and evidence examined can be used by an organization to:

- Identify specific opportunities for improvement in the organization’s ISCM program, including the ISCM strategies;
- Identify the level of understanding within the organization’s leadership or staff of what the ISCM program is and where it fits in the risk management process;
- Identify the level of understanding of how the ISCM program applies to each organizational level and how ISCM functionality is integrated across the entire organization;
- Identify potential opportunities for improvement in the organization’s security and risk management programs, to include linkages from ISCM capability to the organization’s risk management function;
- Prioritize risk response decisions and associated risk mitigation activities related to the organization’s ISCM program;
- Confirm that the organization ensures that identified security-related weaknesses and deficiencies in the systems and in the environment of operation have been addressed;
- Support monitoring activities and information security situational awareness;
- Assess readiness for ongoing authorization; and
- Guide design of a future or planned ISCM program or to evaluate planned modifications to an existing ISCM program.

The foundation of the ISCM program assessment is a set of assessment elements and their usage for making judgments about the ISCM program by the ISCM program assessor. An ISCM program assessment determines whether or how well the ISCM capability meets the requirements and objectives of ISCM as specified by the assessment elements.

The ISCM program assessment leverages the control assessment process performed on common controls, hybrid-controls and system-specific controls. The organization is evaluated on whether it has implemented the control assessment process. This publication does not prescribe the assessment of individual controls nor the examination of control assessment results as part of the ISCM program assessment. Organizations may incorporate additional assessment elements to evaluate the assessment of individual controls or the control assessment process, if desired, as part of the ISCM program assessment tailoring process. The rest of this section explains the components of the ISCM program assessment.

2.2.1 ISCM Program Assessment Criteria

The ISCM program assessment defines the evaluation criteria applied to each aspect of the ISCM program being assessed (e.g., security status monitoring policy and procedures, common control assessment policy, configuration management procedures, security status reporting). The evaluation criteria defined by this publication establish the *assessment element* as the central component. ISCM program assessment elements are statements about various attributes of the ISCM program that are evaluated by the assessor. Each ISCM program assessment element is grounded in one of the six ISCM process steps summarized in Sec. 2.1.2. The complete set of ISCM program assessment elements is presented in the [Catalog] along with the attributes of each element. The following are examples of assessment elements:

- There is an ISCM program derived from the organization-wide ISCM strategy. (Assessment Element 1-002)
- There is organization-wide policy for security status monitoring. (Assessment Element 1-008)
- The procedures for security status monitoring are followed at the documented frequencies. (Assessment Element 3-007)
- There is organization-wide policy for making ISCM results available to the risk assessment process. (Assessment Element 1-011)
- The procedures for determining and prioritizing the responses to risks found by the ISCM program are followed. (Assessment Element 3-023)
- There is a set of ISCM metrics and corresponding review procedures. (Assessment Element 2-024)
- The ISCM strategy is reviewed to identify ways that may improve the ability to respond to known and emerging threats. (Assessment Element 6-005)

ISCM-relevant statements extracted from the sources but that originally spanned more than one ISCM step are expressed as separate assessment elements, one (unique) element for each applicable process step. The assessment elements were also developed from other ISCM functionality and principles, for instance, as suggested by developer, operator, and assessor experience, and from federal guidance.

The [Catalog] provided with this publication is an extensive set of ISCM program assessment elements and is considered to be the minimum set of elements needed for a comprehensive ISCM program assessment. However, an assessment may be limited by the number of ISCM process steps or by the risk management level. Assessment elements that apply to any excluded ISCM process steps are not included in the set of assessment elements presented to the assessor.

Selection of elements depends on the scope of the assessment (explained in Sec. 2.3.2), which may be limited by the risk management level(s) or by the ISCM process step as defined in Sec. 2.1.2. Two examples of limited-scope assessment with selection of assessment elements are:

- For a Level 1-only scope, only elements that apply to Level 1, are selected. Note that elements that apply to Level 1 and Level 2 and elements that apply to Level 1, Level 2, and Level 3 are also included in the set of elements.
- For a scope of only the DEFINE and ESTABLISH ISCM Process Steps, only elements applicable to ISCM Process Steps 1 and 2 are selected from the Catalog or organization-defined set of assessment elements. Note that each element is applicable to only one Process Step, and multiple steps are sequential and include Step 1, DEFINE.

Some assessment elements of the ISCM program assessment are partially outside the scope of the ISCM program. Such elements evaluate use of information from the RMF process (e.g., current risk levels, risk tolerance level, threat and vulnerability information) while other elements evaluate the ISCM program's capability to send security-related information (e.g., security status reports, security metrics) to inform the organization's implementation of the RMF. A few assessment elements may overlap with certain [SP800-53] controls, but the ISCM program assessment does not consider or re-evaluate the effectiveness of individual controls.

The assessment elements and assessment procedures provided with this publication can be used by organizations or assessors as a starting point for developing assessments that produce evidence with the assurance needed to evaluate ISCM programs and determine if ISCM requirements embodied in the assessment criteria are met.

The assessment elements can also be used as requirements for an ISCM program under development. The elements can be used to guide the ISCM program design in terms of functionality, and policies and procedures needed. The elements can also be used to evaluate an ISCM plan or design, such as ISCM technical architecture, operational procedures, and ISCM strategies.

2.2.2 Sources of ISCM Assessment Elements

The sources of ISCM guidance and requirements for elements are:

- Federal Information Security Modernization Act (FISMA) of 2014 [FISMA2014];
- OMB Memoranda addressing ISCM requirements [OMB M-11-33] [OMB M-14-03];
- OMB Circular A-130 (2016) [OMB A-130];
- NIST risk management guidance and ISCM guidance [SP800-37] [SP800-39] [SP800-137];

- Executive Directives, including White House Initiatives and Executive Orders;
- *United States Government Concept of Operations for Information Security Continuous Monitoring, Draft*, Version 2.0; and
- Practitioner experience based on collective professional experience in ISCM, security engineering, network security, systems engineering, and information technology.

The sources are fully attributed in Appendix C and are referenced in the *Source* Attribute column in the [Catalog]. Note that there may be multiple sources from which an assessment element was derived for an ISCM program assessment element.

The ISCM Program Assessment Element Catalog [Catalog] provides 128 assessment elements, each having an assessment procedure and other attributes as part of the element catalog entry. A total of 89 (70 %) of the assessment elements are derived from [SP800-137] and 39 (30 %) from the other listed sources.

2.2.3 Assessment Element Attributes

Each assessment element has attributes to aid in the evaluation of the ISCM program implementation. Attributes are reflected in the Assessment Element Catalog as columns of a table. The following attributes are provided in the [Catalog] for each assessment element:

- Assessment Element ID;
- Assessment Element Text;
- Risk Management Level(s);
- Source;
- Assessment Procedure;
- Discussion – additional guidance relative to the Assessment Procedure attribute;
- Rationale for Level; and
- Parent – linkage to previous Process Step assessment element.

Each ISCM program assessment element has associated guidance in the form of the *discussion* attribute that provides supplemental guidance to assist in the judgment about the assessment element and to clarify possible ambiguities in assessment element wording, potential assessment objects, what to look for with respect to specific objects, and sources of additional information. The discussion attribute and associated guidance is described in Sec. 3.3.

2.2.4 Assessment Element Catalog

The Assessment Element Catalog [Catalog] is an information base in tabular form of all assessment elements defined for the ISCM program assessment. The rows in the Catalog contain the assessment elements with their attributes.

2.2.5 Traceability of Assessment Elements (Chains)

Assessment elements may be linked together to provide traceability from one element to one or more other elements related to the *Parent* attribute and based on a particular aspect of the ISCM program (e.g., security status monitoring or ISCM metrics). Assessment elements linked together to provide traceability are called a *chain*. Chains show the parent/child relationship of elements spanning two or more ISCM process steps.

Assessors may find it beneficial to trace paths through assessment elements by chains as they examine, interview, or test assessment objects at the three organizational risk management levels. For example, one type of artifact or one set of interview questions covering a chain of assessment elements focuses on a narrow subject area (e.g., ISCM strategies), to help assessors make judgments more efficiently.

Figure 2 shows four examples of chains of similar assessment elements, each originating from the *Define* Step (element 1-032). The character string in the upper left corner of each element provides unique identification of an individual assessment element (with the first numeric character being the ISCM process step).

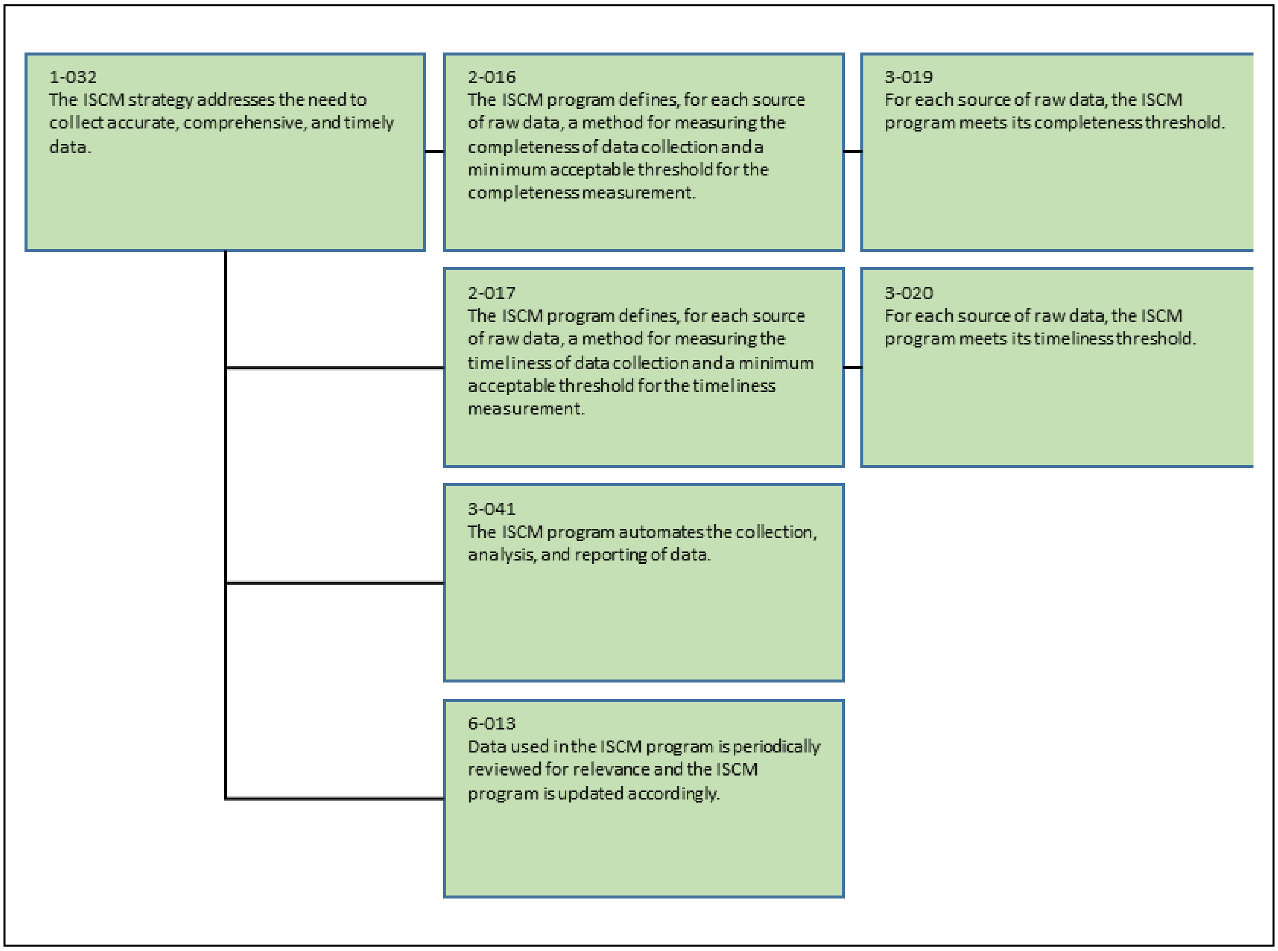

1-032
The ISCM strategy addresses the need to collect accurate, comprehensive, and timely data.
2-016
The ISCM program defines, for each source of raw data, a method for measuring the completeness of data collection and a minimum acceptable threshold for the completeness measurement.
3-019
For each source of raw data, the ISCM program meets its completeness threshold.
2-017
The ISCM program defines, for each source of raw data, a method for measuring the timeliness of data collection and a minimum acceptable threshold for the timeliness measurement.
3-020
For each source of raw data, the ISCM program meets its timeliness threshold.
3-041
The ISCM program automates the collection, analysis, and reporting of data.
6-013
Data used in the ISCM program is periodically reviewed for relevance and the ISCM program is updated accordingly.

Figure 2 – Example of Chains

In the example of four chains in Figure 2, one chain, consisting of assessment elements 1-032, 2-016, and 3-019, links together assessment elements involving the completeness of ISCM-relevant data to be collected. The second chain, consisting of assessment elements 1-032, 2-017, and 3-020, links together assessment elements involving the timeliness of ISCM-relevant data. The third chain, consisting of 1-032 and 3-041, deals with automating this data. The fourth chain, consisting of 1-032 and 6-013, involves using this data in the review and update of the ISCM program.

In following the first chain (1-032, 2-016, and 3-019), the first block is linked to the second, and the second is linked to the third block. An assessor may request artifacts that address the completeness of data collected, as specified in each assessment element of the chain as applicable. The artifacts may then be used to make judgments about all three assessment elements. In following the second chain, the sub-chain 2-017 and 3-020 has the same parent as the first chain (1-032) but is linked based on the timeliness of the data collected, and an assessor may request artifacts that address the timeliness of data collected. As with the first chain, the artifacts may then be used to make judgments about all three assessment elements in the chain, and similarly for the third chain. The assessor may request a demonstration of automated functionality or artifacts documenting automation. For the fourth chain, the assessor may request artifacts illustrating how data is used to evaluate the ISCM program.

Diagrams of the traceability chains are contained in the [Catalog]. These diagrams are arranged by ISCM aspect, such as chains addressing ISCM strategy management, metrics, and control assessment rigor. Assessing elements by aspect (subject), as represented by chains, can yield useful information, particularly when the assessment is scored according to that ISCM aspect, or when deficiencies are to be identified in that aspect of ISCM, such as ISCM-relevant metrics.

2.2.6 Properties of the ISCM Program Assessment

The ISCM program assessment accommodates all aspects of the ISCM program and is grounded in the principles of [SP800-137]. Properties of the ISCM program assessment include:

1. Focusing on one ISCM Process Step at a time.
2. Ensuring each assessment element is applicable to only one ISCM Process Step.
3. Using readily available security-related information (e.g., information specified in the organization-wide or system-level ISCM strategy document).
4. Avoiding re-testing or re-assessing of controls, which is outside the scope of the ISCM program assessment.
5. Assessing the ISCM program's ability to include both automated and manual ISCM methods.
6. Tracing each assessment element to authoritative source(s) or ISCM practitioner experience.
7. Allowing assessors or organizations to add to assessment procedures as necessary, modify the evaluation criteria (which is the Assessment Element Text attribute), or add, exclude, or modify attribute fields of the assessment element, as discussed in Sec. 3.5.

8. Applying to any organization regardless of size and complexity.
9. Maintaining separation and independence from technologies, implementation, and unique organizational or program requirements.
10. Producing results that lead to actionable recommendations.
11. Evaluating from a strategic and programmatic perspective rather than specific, tactical issues detected during ISCM.
12. Including sufficient clarity and guidance that the assessment is repeatable; that is, a follow-up assessment by a different assessment team results in the same outcome.

2.2.7 Assessing the ISCM Program through the Evaluation Criteria

The ISCM program assessment includes a framework for making *judgments*, which are responses made by the assessor to the assessment elements. This section outlines the types of judgments and the ways judgments can be made.

An aspect of the ISCM program, e.g., ISCM strategy or ISCM outputs/reports, is evaluated against a set of assessment elements, which may be a chain of elements as explained in Sec. 2.2.5. For each element considered, a judgment results from the assessor's response in choosing from a set of predefined *judgment values*, examples of which are presented below.

For the set of assessment elements applicable to the scope of an ISCM program assessment, all elements are judged. Sec. 2.3.2 explains scoping of the ISCM program assessment.

2.2.7.1 Judgment Values

Judgment values vary depending on the level of granularity of evaluation the organization needs, and the assessor can achieve. While specific judgment values for an assessment are not prescribed in this guidance, the default judgment value set consistent with NIST guidance is the two-value set, *Satisfied* or *Other than Satisfied* or equivalently, *True/False*.[12]

For the default set of judgments, each determination statement within an assessment procedure (described in Section 3.3) produces one of the following judgments: *Satisfied* or *Other than Satisfied*. The assessment provides for annotations or notes that explain any *Other than Satisfied* judgment, i.e., what portions of an assessment element prevent a *Satisfied* judgment. For example, an annotation can document partially completed ISCM aspects so an organization can track what has been completed and what is lacking. Note that the companion document [Catalog] is established based on the default, two-value set of judgments.

Organizations may also choose to employ a more granular approach to findings by introducing a *Partially Satisfied* category for assessments. Finer-grain annotations can be employed with the two-value judgments to give more precise reasons for *Other Than Satisfied* judgments. (See Sec. 3.3.2 for more detail). Annotations may include a discussion of conditions or situations that do

[12] The two-value judgment set of *Satisfied* and *Other than Satisfied* is aligned with the assessment results used in [SP800-53A].

not yield straightforward judgments. Annotations may be assisted by a tool or may be manually recorded during the assessment.

An example of judgment values with more granularity is:

Mostly/Completely True
Somewhat True
Neither True Nor False
Mostly False
Completely False

In this example, all the judgments are annotatable, even *Mostly/Completely True* where the evidence shows the element is mostly, but not completely true. The organization may use the annotated reasons for the two-value set or a finer granularity set of judgment values to (i.) identify shortfalls; (ii.) indicate what further actions are required to completely satisfy the determination statement; and (iii.) help prioritize potential responses. It is expected that the set of annotations are used to develop the set of recommendations in the assessment results report.

2.2.7.2 Making Judgments

Section 3.3 explains *assessment elements*, which contain guidance on how to arrive at a judgment. The assessment element contains the assessment element text, which is the assessment criteria, and a set of attributes; two of which are the assessment procedure and the discussion used in making judgments. The *assessment procedure* attribute consists of one or more *assessment objectives*, derived from the *assessment element text* and *potential assessment methods and objects*. The *discussion* attribute provides supplemental guidance relevant to the assessment element, and may provide additional detail about special situations or dependencies the assessor may need to consider (see Sec. 3.3).

Once the evidence[13] is obtained or interviews are conducted with the identified potential stakeholders, the assessor makes a judgment if the ISCM program meets a given assessment element. The assessor selects one of the possible judgment values defined for the assessment element as the judgment. The two-value judgment set indicates whether the assessment is satisfied, while the multi-valued, finer grained value set indicates how well the assessment element is met (e.g., *somewhat true, mostly false*).

Figure 3 shows the process for making judgments for an assessment element using the available information.

[13] Examples of evidence relevant to each assessment element are listed in the [Catalog] as potential assessment objects associated with the Examine and Test Potential Assessment Methods.

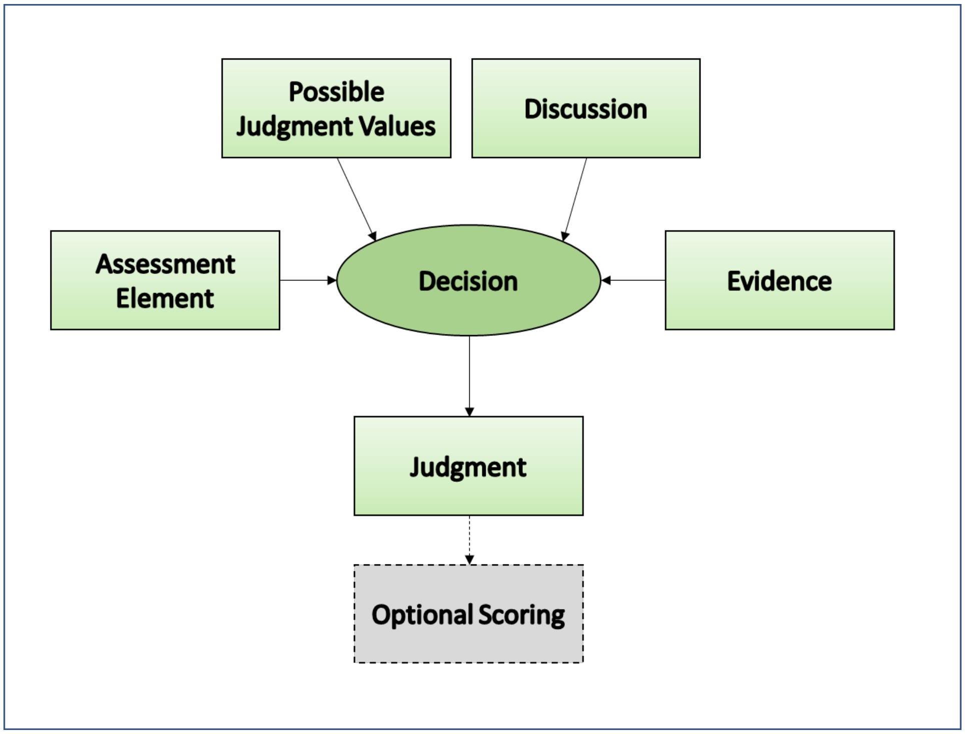


Figure 3 – Process for Making Judgments

2.2.7.3 N/A Judgments

The *Not Applicable* (N/A) judgment is not defined for the ISCM program assessment in this publication. It is important to ensure each assessment element is applicable to the entire organization to the maximum extent, which means that the N/A judgment is not implemented as a judgment value even when some ISCM program assessment functions or aspects are not implemented in the ISCM program (e.g., external service providers are not used), but there are assessment elements to evaluate external service in the assessment.

Since all assessment elements are addressed and are not tailored out of an assessment, the following considerations are relevant to the ISCM program assessment:

- Every assessment element is judged;
- If the subject of an assessment element, such as the use of external service providers, is not applicable to the organization, the organization-wide ISCM strategy specifies that the subject or aspect is not applicable to the organization;
- Regardless of the organizational decision about the subject, the subject is considered and evaluated throughout the ISCM program assessment; and
- The decision not to implement a particular ISCM aspect means that there is no evidence expected to the contrary, which is verified by the assessor.

If an ISCM assessment element is not applicable to the organization or system, it is first addressed in the applicable strategy, and all elements related to that particular subject are judged to be *satisfied*. If the strategy does not address the subject, all elements related to that subject are judged to be *other than satisfied*.

2.2.8 Assessing the ISCM Program within One Organizational Level

Depending on the size and complexity of the organization, ISCM program assessment information may be collected from multiple parts of the organization (e.g., multiple missions/business processes and/or systems), analyzed, and aggregated into a single judgment for a single organizational risk management level. Multiple assessors can produce multiple assessments that are limited in scope to a part of the organization (e.g., a single mission/business process, a single system).

For multiple ISCM program assessments at the same level (i.e., by multiple assessors), the organization or assessors decide how to combine multiple judgments for the same assessment element. Multiple judgments for the same assessment element can occur, for example, if the assessors meet separately with each mission/business process. It is also a result of using a distributed self-assessment, as described in Sec. 2.3.1. There can be significant differences in assessment results across one level. Examples of methods for combining judgments within one organizational risk management level are:

- *Worst case.* The worst judgment (the *low water mark*) is used as the resulting judgment for the level.
- *Majority judgment*. The most common judgment is used as the resulting judgment for the level. If there is a tie for the most common judgment, a predetermined rule is used to determine the resulting judgment, e.g., the worst of the tied judgments.
- *Assessor determined.* The assessor considers all factors and makes an experience-based judgment.

Each assessment element applicable to an assessment is judged for each individual level being assessed as described above.

2.2.9 Assessing the ISCM Program across Multiple Organizational Levels

[SP800-137] describes how the three organizational levels work together to address various aspects of ISCM. The concepts there may apply to one or two levels (usually adjacent levels) or to all three levels, depending on the organizational structure and how the organization-wide and system-level ISCM strategies are applied. As a result, each assessment element is evaluated across one or more levels. For example, one element may be evaluated for Level 1 only, while another is evaluated for Levels 1 and 2. For each element, multiple evaluations are combined into a corresponding *single* judgment regardless of how many levels are being evaluated.

When judgments from two or more levels are combined to get the resultant judgment, a method, rule, or algorithm is needed to ensure that judgments are combined consistently. This publication does not prescribe a means to combine judgments. Each organization defines a combining mechanism that meets its needs.

One or more assessments are conducted for each of the levels involved. Results are combined into a single judgment for each level, as described in Sec. 2.2.8. Results for each of the levels are then reconciled into a single judgment according to organization-defined rules. As an example of a method of combining levels, the following sample rules, based on one of the decision matrices shown in the three figures below, are used:

Rule 1. If the assessment element is applicable to only one level, that level's judgment is the final judgment for the element.

Rule 2. If the assessment element is applicable to exactly two levels, use the decision matrix from Figure 4, Figure 5, or Figure 6.

Rule 3. If the assessment element is applicable to all three levels:

a. Apply Rule 2 to Levels 2 and 3; then

b. Apply Rule 2 to Level 1 and the result from Rule 3a.

Note that it is not necessary to use a decision matrix with any of the rules above. A simple rule may be used instead, such as, *when combining two judgement values, select the worst-case value as the resultant judgment* (or select the majority judgment[14] or use another method).

Table 1 shows an example decision matrix an assessment may use for combining two levels of judgments using Rules 2 or 3 above. In this example, the approach for combining two levels having different values is to apply the *worst*-case method, which results in an *Other than Satisfied* judgment in three of the four cases.

Table 1 – Combining Judgments from Two Levels (Unbiased) [15]

Lower Level	Higher Level	Combined Judgment (Unbiased)
Satisfied	Satisfied	**Satisfied**
Satisfied	Other-than-Satisfied	**Other-than-Satisfied**
Other-than-Satisfied	Satisfied	**Other-than-Satisfied**
Other-than-Satisfied	Other-than-Satisfied	**Other-than-Satisfied**

Table 2 presents an alternative matrix for combining two levels that gives priority to the higher level, which has a broader view of the actual business of the organization. Rules 2 and 3 remain the same using the matrix of Table 2. However, the outcome of applying any of the rules is different from the outcome of the Table 1 matrix.

[14] Based on judgments obtained for one or both levels assessed.

[15] The words higher and lower refer to the positions within the risk management hierarchy, as described in [SP800-39]. The highest level is Level 1, the lowest level is Level 3.

Table 2 – Combining Judgments from Two Levels (Higher level bias)

Lower Level	Higher Level
Satisfied	Satisfied
Satisfied	Other-than-Satisfied
Other-than-Satisfied	Satisfied
Other-than-Satisfied	Other-than-Satisfied

Table 3 presents another alternative matrix for combining two levels that gives priority to the lower level, which may be closer to what is actually occurring in the organization. Rules 2 and 3 remain the same with the matrix of Table 3. However, the outcome of applying any of the rules is different from the matrices of Tables 1 and 2.

Table 3 – Combining Judgements from Two Levels (Lower level bias)

Lower Level	Higher Level	Combined Judgment (Lower level bias)
Satisfied	Satisfied	**Satisfied**
Satisfied	Other-than-Satisfied	**Satisfied**
Other-than-Satisfied	Satisfied	**Other-than-Satisfied**
Other-than-Satisfied	Other-than-Satisfied	**Other-than-Satisfied**

2.2.10 Scoring

Within an assessment, scores indicate how well the ISCM capability meets its objectives and reflect risk to the organization. Judgments made using the assessment elements may be assigned a score, which is a numerical value representing the judgment that can then be used to calculate assessment results. Scores are assigned to each judgment value and the resultant score for the organization is computed using the scores of each assessment element. That is, the assessment score is the sum of all the element judgment scores.

The scores may facilitate informed decision-making by organizational leadership regarding the ISCM program and where organizational resources can best be applied to improve the program to reduce risk. Scoring is optional and may be used with the binary and multi-gradation judgment types discussed in Sec. 2.2.7. Scoring may also be used to aggregate ISCM program assessment scores from across the organization into a single, summary score for the entire organization.

Using the default binary judgment values, each assessment element is assigned one of two possible scores. For example:

Table 4 – Example of Default Judgment Value Scoring

Score	Judgment
1	Satisfied
0	Other than Satisfied

An assessment element score can optionally be multiplied by a weighting factor, which is a numerical value that results in a higher score for that assessment element. Different weights can be assigned to different assessment elements based on the criticality of a given element to an organization. In other words, an organization may create a scheme of weight assignments, i.e., multiple weight factors for multiple priorities of differing importance. Section 2.2.11 explains factors that may affect the criticality of an assessment element.

As with any type of numeric scoring, the result can be expressed as a percentage by dividing the score by the best possible score.

2.2.11 Criticality

Assessment elements can be identified as critical or non-critical, which may impact how the elements are scored. ISCM program assessment elements may be deemed critical under the following conditions:

- The ISCM program addresses, for example, the following:
    - National cybersecurity concerns, e.g., protecting high-value asset (HVA) information and systems;
    - Serious and pervasive security issues across the Nation, the organization, or a given sector, such as insider threats;
    - National cybersecurity initiatives, e.g., transition to ongoing authorization, presidential cybersecurity initiatives; and
    - Proprietary issues that affect the business processes or mission(s) of the organization.
- One part of the ISCM program provides a foundation for the remainder of the program thereby making the evaluation of certain assessment element(s) important, e.g., ISCM strategies, policies, and procedures are important in evaluating the implementation and/or operation of the ISCM capability;
- The ISCM program is a part of other important commercial needs or national cybersecurity programs or initiatives, e.g., the RMF or Cybersecurity Framework (CSF) [CSF 1.1]; and
- The ISCM program covers a broad area of cybersecurity functionality or responsibility, e.g., common controls.

Over the lifetime of an assessment, the designation of critical assessment elements may change to reflect new national cybersecurity priorities and goals and cybersecurity issues. In addition, critical assessment elements may vary from one organization to another depending on factors such as the organization’s risk tolerance.

2.2.12 Reporting of Assessment Results

If scoring is performed, ISCM program assessment results include the scoring results for each assessment element combined into a single score for the organization or for the part of the organization being assessed. Reports may be broken out by overall organization, individual organizational parts, organizational level, or specific assessment element attributes such as source of assessment element, various aspects or categories (e.g., strategy, metrics, governance, criticality of findings), individual scores by assessment element, or other grouping meaningful to the organization.

Assessment results include recommendations based on the data collected and analyzed. Some recommendations are formed automatically from judgment results, with potential assistance from an assessment tool, while others are made by a manual decision process by the assessors. Organizations or third-party assessors optionally add their own recommendations based on their considerations of the assessment element judgments.

Assessment results can be presented in the assessment report in several different ways depending on the intended use; for example, radar charts, diagrams, and tables summarizing results of judgment. Results can also be incorporated in displays of assessment scores that give various views of the results. Results in the form of metrics may be reported to various organizational officials (e.g., CIO, SAISO, RE(F), AO) where they may be used to inform risk-based decisions.

2.3 Using the ISCM Program Assessment

The overarching goal of the ISCM program assessment is to provide organizations with recommendations to improve the ISCM program, and thereby manage and reduce organizational risk. There are different ways to characterize the ISCM program assessment process, including type of assessment and type of assessors, depth and duration of the assessment, and expected results of the assessment.

2.3.1 Conducting the ISCM Program Assessment

There are two types of ISCM program assessment engagements: third-party assessments and self-assessments.

Third-party assessments. Third-party assessments are conducted by third-party assessors who are separate and independent of the organization being evaluated. Third party assessments may be:

- External – Assessors are employed from outside organizations and are independent[16]; and
- Internal – Assessors are part of the organization but are considered to be independent of the organizational entity under assessment for the assessment task.

[16] Assessor independence is a factor in preserving an impartial and unbiased assessment process; determining the credibility of the assessment results; and ensuring that organizational officials receive objective information to make informed, risk-based decisions.

Third-party assessments are usually conducted over more than one session and are usually facilitated as follows: the responses from a set of participants are discussed, then the consensus response is decided and noted, such as by entering it into a tool or repository of results by the assessors.

Self-assessments. Self-assessments may be conducted by the staff of the organization or sub-organization being evaluated. Self-assessments rely on an objective view of the target and can inform the organization or part of the organization of shortcomings in the ISCM capability early in the ISCM program development.

The self-assessment may be conducted as a distributed assessment, where:

- An internal staff member leads the participants independently as they evaluate the assessment elements in parallel; and
- The responses from a set of assessors are entered directly into a tool or repository by the participants, possibly at different times, and then the overall response is calculated by the tool or manually (or by a semi-automated procedure), without discussion, after the responses are collected.

Alternatively, the self-assessment may be conducted like a facilitated assessment where one staff member or team with subject matter expertise facilitates discussion in a group, then the consensus response is decided and noted, such as by entering it into a tool or repository of results.

2.3.2 Extent and Duration of ISCM Program Assessments

The extent of the ISCM program assessment is flexible in terms of which process steps it addresses. The assessment can stop at any step or logical stopping point or can evaluate a portion of an organization rather than the entire organization. The ISCM program assessment has the following characteristics that define the ISCM program assessment scope:

- The ISCM *Define* step is always included to ensure the foundation of ISCM is evaluated; and
- The ISCM program assessment can be conducted incrementally and halted after any step. For example, the assessment can:
    - Stop at the *Define* Step (focus on ISCM program strategy(ies));
    - Stop at the *Establish* Step (focus on ISCM program design);
    - Stop at the *Implement* Step (focus on ISCM implementation);
    - Exclude the *Review/Update* Step (a process improvement step that reflects a relatively mature ISCM program); or
    - Include all Steps (a full ISCM program assessment).

The ISCM program assessment is flexible enough to allow an assessment to be suspended temporarily at a specific point. Assessment suspension may be beneficial for various reasons, e.g., to make improvements to the ISCM program before continuing. If desired, the assessors may assist the organization to address shortcomings found.

2.3.3 Expected Outcomes of ISCM Program Assessments

The expected outcome of the ISCM program assessment is improvement of the security posture of the organization and risk reduction. To this end, the ISCM program assessment produces actionable recommendations to improve the ISCM program, such as, in the areas of ISCM program design, implementation, operation, and governance. The primary output of the ISCM program assessment is an ISCM program assessment report of findings to the organization. The ISCM program assessment report includes the following, as applicable:

- Introductory and background material, e.g., overview of the assessment process;
- Detailed scorecard (if scoring is used) and/or other visualizations that summarize the organization's ISCM program effectiveness;
- Specific ISCM areas that are implemented well, based on assessment criteria;
- Specific ISCM areas that can be improved; and
- Specific recommendations on how to make ISCM improvements and how those actions will improve the ISCM scorecard.

In addition, a separate report on the engagement may be made to the assessment organization by the evaluated organization's staff with the objective of improving the ISCM program assessment process.

3 The Process

This section describes the component parts of an assessment and the overall ISCM program assessment process. The ISCM program assessment process defines how to evaluate the organizational ISCM capability including: (i) the activities carried out by organizations and assessment bodies to prepare for ISCM program assessments; (ii) the development of the ISCM program assessment plan; (iii) the conduct of ISCM program assessments and the analysis and reporting of assessment results; and (iv) post-assessment report analysis and follow-on activities.

3.1 Overview of the ISCM Program Assessment Process

A successful ISCM program assessment requires the consideration of the needs of all parties having a vested interest in the organization's ISCM capability, including system owners, authorizing officials, chief information officers, chief information security officers, senior agency officials for privacy/chief privacy officers, chief executive officers/heads of agencies, security and privacy staff, Inspectors General or other auditing bodies, the risk executive (function), and the senior agency official for risk management. Establishing an appropriate set of expectations before, during, and after an assessment is paramount to achieving an acceptable outcome – that is, producing information necessary to help the organization's leadership make an informed decision about whether the ISCM program is adequate to meet the organization's needs. The decision may impact authorization decisions to place a system into operation or continue its operation (ongoing authorization). Figure 7 shows the overall process, and details are described in subsequent sections.

While an assessment relies on a manual process implemented by assessors, it leverages input from automated ISCM processes as evidence to be used in making judgments. For example, ISCM-produced reports may be supplied to the assessor by an organizational dashboard or security information and event management (SIEM) component; the assessor then uses the ISCM-produced reports to make judgments against one or more specific assessment elements. The assessor (or a tool, if available) then collects and aggregates judgment results from assessment participants at all applicable levels to produce an organization-wide judgment, which is the basis for the assessment findings.

The ISCM program assessment developed under guidance of this publication evaluates the ISCM program itself, not the results of the operational ISCM program. The ISCM program assessment does not have the objectives of: (i) retesting security control effectiveness or operational procedures; (ii) evaluating ISCM implementations; or (iii) validating specific outputs of the ISCM program. The ISCM program assessment does not generally review results of individual control assessments, but rather verifies that control assessments are performed in accordance with the ISCM strategy at the organization-specified frequencies for all parts of the organization under assessment.

Repeatability of the ISCM program assessment process is a desirable property to help ensure consistency in results. The guidance in this publication, through the use of the ISCM program assessment elements described in Sec. 3.3, helps to ensure repeatability in conducting assessments by providing assessor guidance on potential assessment objects to examine, what to look for during the examination, the assessment objective for evaluating each individual assessment element, and the personnel roles to interview. In addition, the discussion attribute of the each ISCM assessment element provides guidance on how to make judgments about assessment elements and may specify the valid judgment values the assessor can select.

Section 3.5 addresses how the organization or assessor may tailor the approach presented in Sec. 3 to achieve an assessment that meets organizational and assessor needs.

> An ISCM program assessment is focused directly on evaluating the ISCM program, as defined and implemented within the organization, and not on evaluating the individual lower-level components of an ISCM capability, such as individual common, hybrid- and system-specific controls. The ISCM program assessment verifies the existence of the subject of the assessment element (for example, to verify that specified procedures for performing certain actions at specified frequency(ies) are followed). The ISCM program assessment does not evaluate individual automated, manual, or operational functions of the ISCM capability.

3.1.1 ISCM Program Assessment Plan

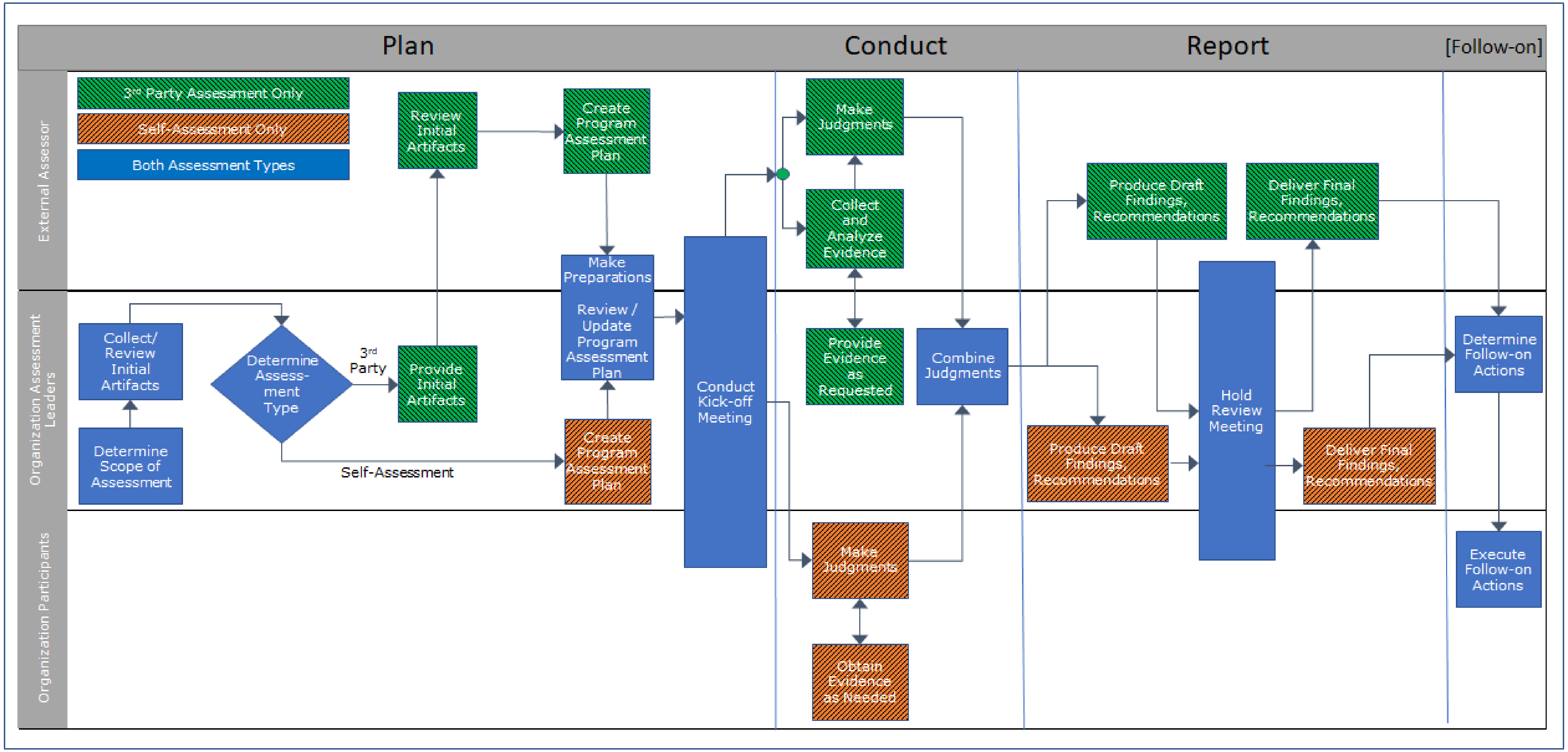
The ISCM Program Assessment Plan guides the execution of the ISCM program assessment. The ISCM Program Assessment Plan documents decisions made during the Plan step of the ISCM program assessment process (as described in Sec. 3.2) and is developed as follows:

- For a third-party assessment, the assessing team creates the ISCM Program Assessment Plan and submits it to the organization for review and approval. The final version is presented to assessment participants at the kick-off meeting.
- For a self-assessment, the ISCM Program Assessment Plan is developed internally to the organization by key assessment staff and organization management. The ISCM Program Assessment Plan is approved by organizational leadership, who will act upon the results of the ISCM program assessment. The final version of the ISCM Program Assessment Plan is presented to the assessment participants at the kick-off meeting.

The ISCM Program Assessment Plan specifies, but is not limited to, the following:

- Type of assessment;
- Scope of assessment;
- Source of staffing;
- Assessor roles;
- Schedule and timeframe;
- Key milestones;
- Activities to be performed sequentially and concurrently;
- Methods for combining assessor judgments across one organizational risk management level;

- Methods for combining assessor judgments across multiple organizational risk management levels;
- Logistics information;
- Assessment tailoring decisions and implementations; and
- Type of report (draft report and final report).


Plan
Conduct
Report
[Follow-on]
External Assessor
Organization Assessment Leaders
Organization Participants
3rd Party Assessment Only
Self-Assessment Only
Both Assessment Types
Review Initial Artifacts
Create Program Assessment Plan
Make Preparations
Review / Update Program Assessment Plan
Collect/ Review Initial Artifacts
Determine Assess-ment Type
3rd Party
Provide Initial Artifacts
Determine Scope of Assessment
Self-Assessment
Create Program Assessment Plan
Conduct Kick-off Meeting
Make Judgments
Collect and Analyze Evidence
Provide Evidence as Requested
Combine Judgments
Make Judgments
Obtain Evidence as Needed
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Hold Review Meeting
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Determine Follow-on Actions
Execute Follow-on Actions

1192

1193 **Figure 4 – ISCM Program Assessment Process**

3.2 ISCM Program Assessment Process Step

The ISCM program assessment is conducted by means of an engagement process, which is a logical, methodical approach to the assessment, based upon existing assessment approaches. There are three steps in the ISCM program assessment process:

- Planning for the ISCM program assessment (Plan);
- Conducting the ISCM program assessment (Conduct); and
- Reporting the results of the ISCM program assessment (Report).

Each ISCM program assessment engagement is tailored based on the needs of the organization and the applicable assessment elements. The ISCM program assessment may be a self-assessment or a third-party assessment, as explained in Sec. 2.3.1. Figure 4 illustrates the activities within each of the three major engagement steps of the ISCM program assessment.

3.2.1 Plan Step

The Plan Step of the ISCM program assessment defines the assessment process and formalizes the conduct of a program assessment as illustrated in Figure 5.

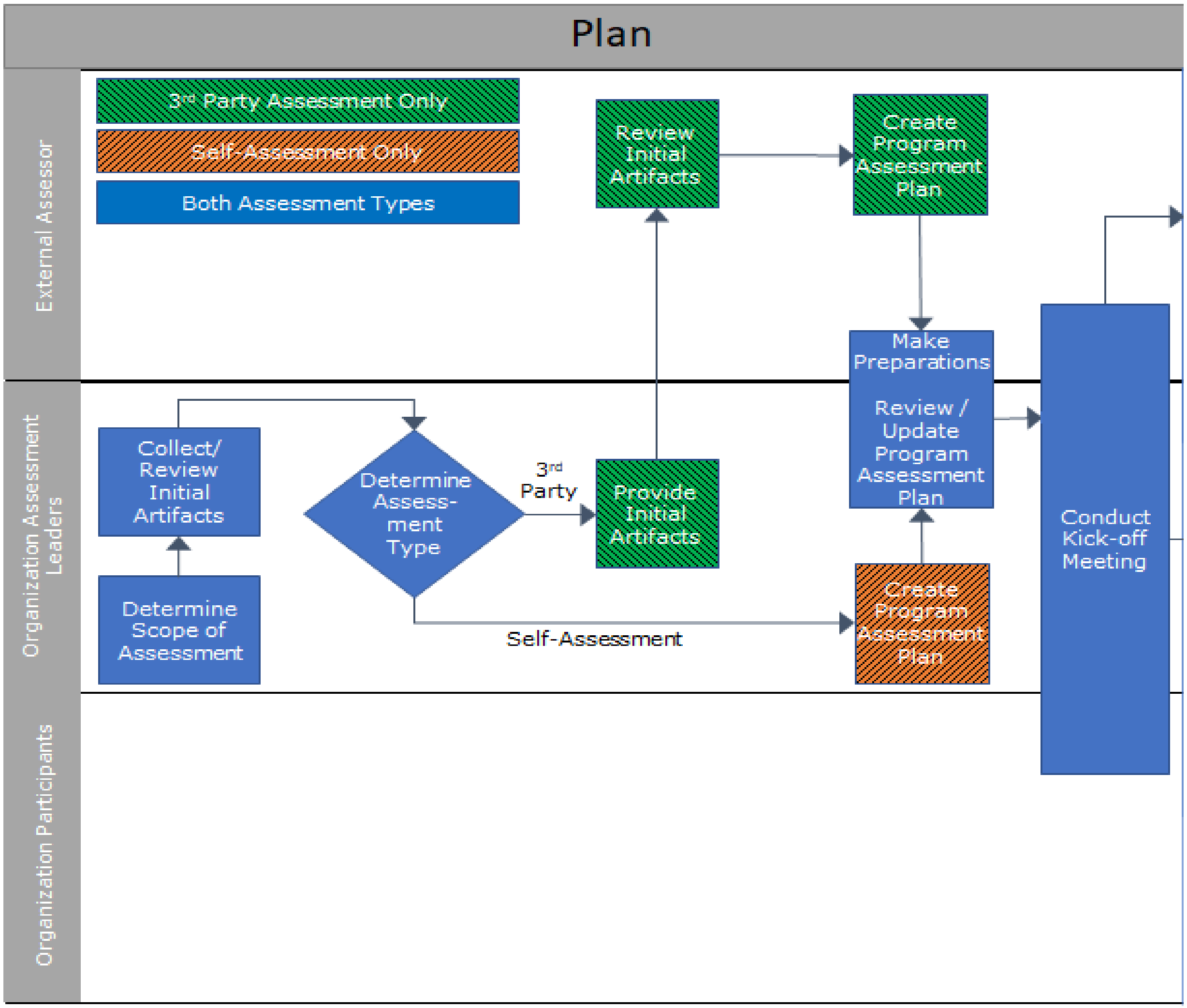

Plan
External Assessor
Organization Assessment Leaders
Organization Participants
3rd Party Assessment Only
Self-Assessment Only
Both Assessment Types
Review Initial Artifacts
Create Program Assessment Plan
Make Preparations
Review / Update Program Assessment Plan
Conduct Kick-off Meeting
Collect/ Review Initial Artifacts
Determine Scope of Assessment
Determine Assess-ment Type
3rd Party
Provide Initial Artifacts
Self-Assessment
Create Program Assessment Plan

Figure 5 – ISCM Program Assessment Process (Plan)

Planning activities address a range of important issues relating to the type of engagement (self-assessment or third-party assessment), cost, schedule, staffing, and logistics of the ISCM program assessment. Planning assumes that each assessment element is applicable to one or more organizational levels. A judgment about an element is made by participants from only one applicable level, *independently* from the judgments made by participants at any other applicable level.

To achieve a comprehensive ISCM program assessment, assessment leaders ensure all areas of ISCM to be considered are evaluated by knowledgeable staff, as follows:

- The team conducting a third-party ISCM program assessment includes staff knowledgeable about all the capabilities included in the ISCM program assessment scope. It also includes, or has reach back to, individuals with operational experience in the various areas of the ISCM program assessment. The relevant skills and experiences are necessary to provide accurate and consistent judgements, and meaningful recommendations for improvement.

- The individuals conducting a self-assessment are knowledgeable about their specific area of ISCM.

Prior to detailed planning, it is helpful to review an initial set of foundational artifacts (e.g., the organization-wide ISCM strategy and an organization chart). Then, based upon relevant information from the initial set of artifacts, the ISCM Program Assessment Plan is updated to adjust the following, for example:

- Degree of engagement at the organization;
- Assessment objects to be examined and personnel to participate;
- Time frames for completing the ISCM program assessment;
- Key milestone decision points required by the organization to effectively manage the assessment; and
- Activities to be conducted serially and in parallel.

The organization performs the following key planning activities:

- Obtaining the organization's approval for the ISCM program assessment;
- Establishing the objective, rigor, and scope of assessment;
- Ensuring leadership of the organization understands the mission/business processes to be assessed, and the mission/business processes are sufficiently organized so that assessors can acquire needed information to evaluate relevant assessment elements;
- Notifying key organizational officials of the impending ISCM program assessment and allocating necessary resources to carry out the assessment;
- Planning the kick-off meeting;
- Ensuring ISCM-relevant artifacts are available to assessors (e.g., documented policy and operational procedures, plans, specifications, designs, records, ISCM reports, system documentation, information exchange agreements, previous assessment results, legal requirements); and
- For a self-assessment, identifying and selecting knowledgeable assessors/assessment teams from the organization, considering issues of assessor independence.

As part of establishing the scope of the assessment, the organization may determine that a partial assessment (as described in Sec. 2.3.2) is appropriate; that is, the plan may limit the number of process steps or parts of the organization to be assessed. Once the engagement has been approved by the organization, relevant artifacts are provided to the assessment team which decreases the assessment duration by enabling the team to examine detailed background information prior to the kick-off meeting.

The assessment team begins preparing by:

- Meeting with appropriate organizational officials to ensure common understanding for assessment objectives, proposed rigor, and scope of the ISCM program assessment;

- Establishing appropriate organizational points of contact needed to carry out the ISCM program assessment;
- Obtaining a general understanding of the organization's operations (including organization structure, mission, functions, business processes, and staff roles);
- Identifying any priority areas (e.g., problem areas, high priority/visibility initiatives), on which to focus the ISCM program assessment;
- Obtaining a general understanding of how the systems within a mission/business process support that process;
- Obtaining an understanding of the structure of each system (i.e., system architecture to be reviewed); and
- For a third-party assessment, identifying and selecting competent assessors/assessment teams, and considering issues of independence if the assessors are part of the organization (i.e., an internal third-party assessment).

Organization and assessment leadership jointly perform the following activities:

- Plan and prepare for a kick-off meeting between organizational leadership and the assessors; and
- Establish communication between the organization and the assessors to minimize ambiguities or misunderstandings about the implementation of ISCM and any weaknesses/deficiencies identified during the ISCM program assessment.

A kick-off meeting is conducted to confirm engagement decisions, answer questions, address additional issues, and resolve any logistical issues. Attendees of the kick-off meeting include the following organizational personnel: organizational senior leaders (CIO, SAISO/CISO, RE(F)), mission/business owners, system owners, system security officers, other staff selected to participate in or support the ISCM program assessment, and administrative support staff to include logistics and facility points of contact. The following personnel from the assessment organization also attend the kick-off meeting: assessment organization leaders and senior assessor personnel.

3.2.2 Conduct Step

The ISCM program assessment is conducted according to the ISCM Program Assessment Plan, which may have been modified during the kick-off meeting. The availability of artifacts, as well as access to organization personnel, relevant to the ISCM program and the systems in scope for the assessment are paramount to a successful ISCM program assessment. Figure 6 illustrates the Conduct Step of the ISCM program assessment process.

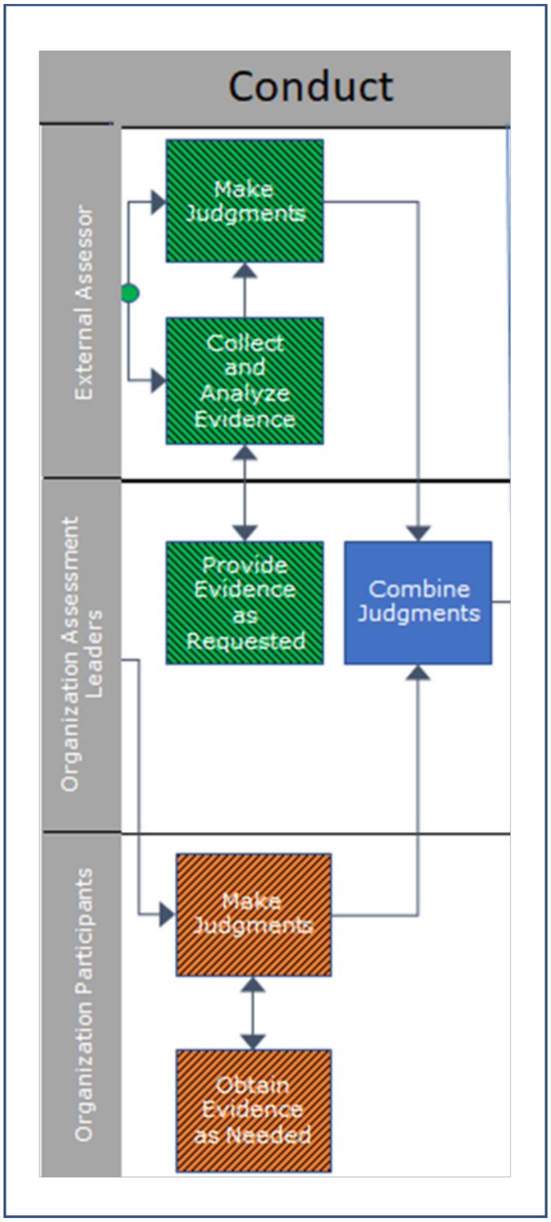

Conduct
External Assessor
Make Judgments
Collect and Analyze Evidence
Organization Assessment Leaders
Provide Evidence as Requested
Combine Judgments
Organization Participants
Make Judgments
Obtain Evidence as Needed

Figure 6 – ISCM Program Assessment Process (Conduct)

The goal of the Conduct Step is to understand how well the organization's ISCM program:

- Plans, creates an organization-wide ISCM strategy, and establishes the ISCM program;
- Plans and implements optional mission/business process ISCM strategies;
- Plans and implements system-level ISCM strategies for all systems within each specific mission/business process being assessed;
- Implements, operates, and sustains the ISCM capability;
- Analyzes ISCM results to determine organizational security posture;
- Responds to ISCM results to reduce organizational risk;

- Informs all levels of the organization of ISCM results;
- Detects gaps and shortcomings in the monitoring of implemented controls at the organization-specified frequency to determine if the controls are effective in meeting their intended purpose; and
- Reviews, updates, and improves the ISCM program.

Basic spreadsheet, presentation, and word processing technologies are available and useful to maintain and present the body of assessment elements and raw data from the assessment to assessors and organization leadership. There may be commercially available tools that are oriented toward system and organization program assessments based on specific assessment criteria that can be used to support an assessment; however, this publication does not endorse any commercial information technology products, applications, or systems.

Organizations can deploy tools to meet assessment needs and can use the assessment elements in this publication as the basis of an assessment tool, including use of assessment elements as the requirements base of a tool.[17] Assessment tools can be developed to support judgment decisions including collaboration methods, Delphi model, voting by assessors, and surveying knowledgeable personnel.

3.2.2.1 Evidence Gathering

ISCM program assessment information is obtained from organizational staff and ISCM outputs (reports) rather than interacting directly with the ISCM capability. Interviews are conducted with personnel from all organizational levels based on organization structure, roles, and scope of assessment to capture relevant information and to make judgments about assessment elements.

While automation is the primary method of collecting ISCM security-related information about control effectiveness, some controls are monitored manually, and thus the ISCM program assessment also obtains ISCM results produced from manually collected data. The evidence obtained for the ISCM program assessment includes, but is not limited to:

- Documents:
  - Organization-wide ISCM strategy;
  - Organization-wide ISCM policy (may be separate or included in the ISCM strategy);
  - Optional mission/business process ISCM strategies;
  - System-level ISCM strategies;
  - Operational ISCM implementation processes; and
  - System security plans.
- ISCM-produced security related information from:

[17] One such tool is ISCMAx, which is included in [NISTIR8212].

- Reports produced by dashboard(s) or other dynamic monitoring systems and components (e.g., SIEMs);
- Reports produced manually; and
- Reports produced for leadership at all three levels, to include reports to CIO, CISO, risk executive (function) staff, AOs, mission and business area management, common control providers, system owners, and ISSOs.

- Human insight obtained from:
    - Interviews with organizational leadership;
    - Interviews with system owners and system security officers;
    - Interviews with system administrators;
    - Interviews with risk management officials; and
    - Interviews with authorizing officials.

If appropriate, previous ISCM program assessment results may be reused as part of the information for the current ISCM program assessment (e.g., Inspector General reports, audits, vulnerability scans, physical security inspections, prior security or privacy assessments, developmental testing and evaluation, and vendor flaw remediation activities).

3.2.2.2 Evidence Analysis

Collected information is manually analyzed by the assessment staff and findings are entered into the repository or assessment tool being utilized, which may be capable of creating graphs and charts. Information analysis leads to judgments about the degree to which the ISCM program meets each relevant assessment element.

Judgments are made at each organizational level to decide the ISCM program adequacy for a given assessment element at that level. If there are multiple judgments made at one level by individuals or groups working in parallel, the judgments are aggregated into a single judgment for that level by the assessor, as described in Sections 2.2.8 and 2.2.9. For example, an assessor may aggregate judgments made at the system level into a single judgment encompassing all judgments about all systems assessed for a particular assessment element.

As the ISCM program assessment engagement progresses, the assessors review artifacts, interview staff, and analyze information gathered. Each day may end with a short discussion with the appropriate organization contacts to clarify and confirm any findings, ask any further questions, and confirm activities for the following day.

System-level ISCM program assessments can be conducted by or supported by system developers, system integrators, security control assessors, system auditors, system owners, the security staffs of organizations, and AOs and AO staff. The ISCM program assessors bring together available information about each system under review. If necessary, assessors conduct enhanced system-level assessments by modifying assessment procedures and methods within the assessment element to collect additional or unique information about systems with respect to the ISCM program.

Mission/business process ISCM program assessments can be conducted or supported by mission/business owners, common controls providers, security control assessors, and CISO staff security specialists. The organization-wide ISCM program assessment can be conducted or supported by staff of the organization's CIO and SAISO/CISO, and risk executive (function).

Once there is a single judgment about an assessment element from each applicable organizational level, the judgments are combined as necessary into a single judgment for a given element. When all elements have a single judgment, the Conduct Step concludes.

3.2.3 Report Step

The Report Step (Figure 7) is the last step of the engagement process that includes participation by the assessors. The Report Step of the ISCM program assessment defines the output-oriented part of the ISCM program assessment.

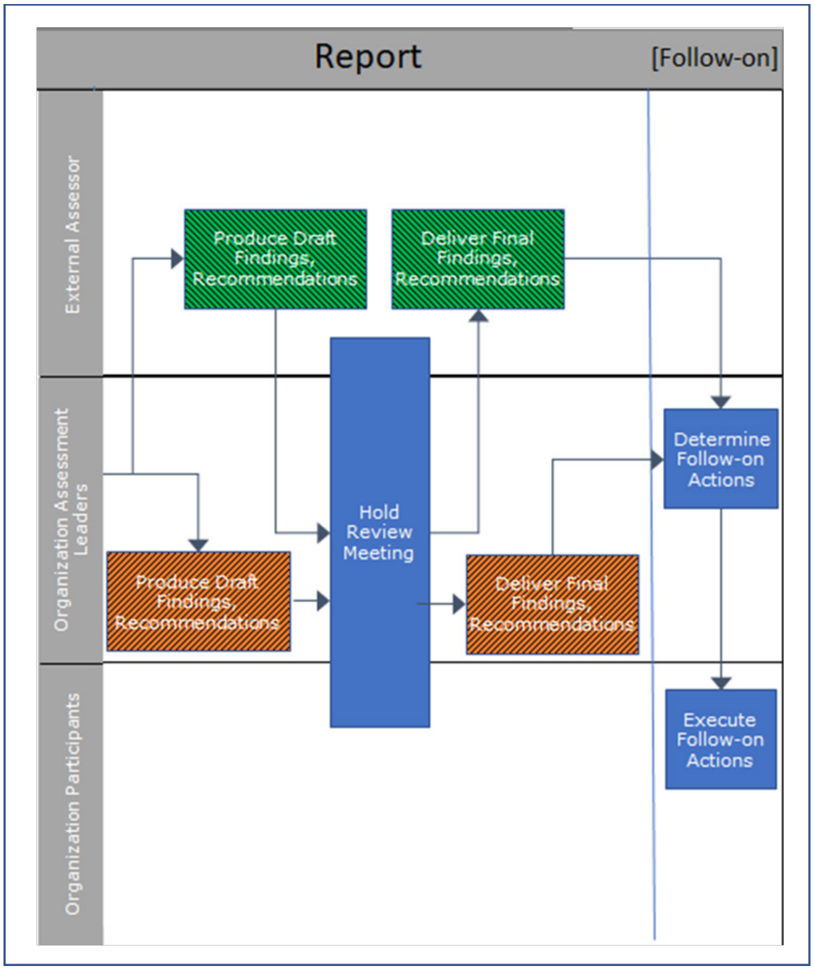

Report
[Follow-on]
External Assessor
Organization Assessment Leaders
Organization Participants
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Hold Review Meeting
Determine Follow-on Actions
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Execute Follow-on Actions

Figure 7 – ISCM Program Assessment Process (Report)

During the Report Step of an engagement, assessors create a draft report of the assessment findings. ISCM program assessment conclusions are manually made by the assessors based on the analyzed information. Assessors make recommendations for improving ISCM programs based on the conclusions from the ISCM program assessment, as may be documented in the annotations for assessment judgments that are not *satisfied* (or True). The assessment process produces qualitative results and recommendations, to assist the organization in focusing subsequent efforts to improve the ISCM program. The organization is given a draft report of findings and recommendations. The draft report is reviewed by organizational leadership to correct any errors and to clarify misunderstandings or ambiguities. Based on feedback from the organization, the assessor produces an updated, final report. The ISCM program assessment report is described in Sec. 2.2.12.

3.2.3.1 Post Assessment Response (Follow-on Actions)

The organization is accountable for responding to ISCM program assessment findings. The organization analyzes the findings in the ISCM program assessment final report, determines the appropriate responses, prioritizes response actions in accordance with organizational risk tolerance, and assigns the role(s) responsible for executing response actions and a time frame for completion. Planned response actions may be documented in system-, mission/business process-, or organization-level plans of action and milestones or in an organization-defined format. ISCM program-related documents (ISCM strategies, policies, etc.) are also updated to reflect any changes resulting from findings and organizational response to findings. Organizations may also validate completed response actions by having the related ISCM program assessment element(s) reassessed.

3.3 ISCM Program Assessment Elements

The ISCM program assessment element defines the evaluation criteria applied to each aspect of the ISCM program being assessed. In order to determine if an ISCM program assessment element is satisfied, assessors use the associated assessment procedure to obtain and review evidence. The assessment procedures apply to the same organizational levels as the assessment elements.

When an ISCM program assessment element is added or modified for a specific assessment of the organization, the corresponding assessment procedure information is created or modified. Other attributes, such as discussion, are also added, or modified. Section 3.5 explains tailoring the ISCM program assessment process, to include tailoring the assessment elements.

The ISCM program assessment elements promote repeatability of the ISCM program assessment process and offer the necessary flexibility to customize assessments based on scope, organizational structure, policies and procedures, operational considerations, system and network architecture, and tolerance for risk.

3.3.1 Assessment Element Information Fields

The information fields of the assessment element, including contextual information or attributes[18] of the assessment element, are defined below.

[18] In the [Catalog], attributes are the cells of each row of the (catalog) table.

Identifier. A string that uniquely identifies the assessment element and indicates the ISCM step number (see Sec. 2.1.2) and a sequence number.

Assessment Element Text. Defines the evaluation criteria applied to an aspect of the ISCM program being assessed. The text of the assessment element is a statement about which the assessor determines whether, or how well, the statement is met.

Level. The applicable organizational risk management level(s) defined in [SP800-39]. See Sec. 2.1.3 for more information about applying the ISCM assessment element to organizational risk management levels.

Source. Authoritative publications or practices from which the ISCM program assessment elements are derived.

Assessment Procedure. The assessment procedure is a multi-part attribute specifying a set of actions to be carried out on evidence gathered by the assessor to determine if an assessment objective has been met. Each assessment procedure consists of (i) an assessment *objective,* (ii) a set of potential assessment *methods,* and (iii) assessment *objects* that are used to conduct the ISCM program assessment as follows:

> **Assessment Objective**. Each assessment objective includes a determination statement related to the assessment element text. The determination statement (i.e., "Determine if" …) refers to the content of the assessment element text and determines whether or how well the evaluated aspect of the ISCM program meets the underlying ISCM principle or requirement specified in the applicable source for that element. The application of an assessment procedure to an aspect of the ISCM program under evaluation produces an assessment *finding*, which reflects whether or how well the assessment element is met.
>
> **Potential Assessment Methods and Objects.** The assessment procedure contains a specification of the suggested assessment methods and the objects to which the methods are applied. The assessment method defines the nature and the extent of the assessor's actions. The potential assessment methods are:
>
> - *Examine:* The process of reviewing, inspecting, observing, studying, or analyzing one or more of the assessment objects. The purpose of the *examine* method is to facilitate understanding, achieve clarification, or obtain evidence.
> - *Interview*: The process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.
> - *Test*: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The assessment *test* method may duplicate system testing that has already been conducted in implementing an organization's ISCM capability. In certain situations, for instance, testing related to technical control effectiveness may need to be conducted if the ISCM program assessment requires such testing as evidence. The approach here assumes that the *test* assessment method is not generally necessary.

The organization and the assessor coordinate with respect to the evidence needed to provide the level of assurance[19] about ISCM program effectiveness desired by the organization. In all three assessment methods, the evidence is used in making specific determinations called for in the determination statements to confirm the objectives of the assessment procedures.

Assessment objects are the potential items (evidence) to which an assessment method is applied. Assessment objects can include specifications, mechanism outputs, activities, and individuals that help the assessor make judgments about whether or how well the assessment element is satisfied by an aspect of the ISCM program. Specifications are document-based artifacts, for example:

- ISCM strategies;
- ISCM program policies and procedures;
- system security plans;
- security requirements;
- ISCM automation functional specifications; and
- ISCM technical architecture designs.

Mechanism outputs are reports or notifications from specific hardware, software, or firmware monitoring functions or safeguards employed within a system or operating environment, for example:

- security dashboard reports;
- SIEM reports; and
- network firewall reports.

Activities are the monitoring-related actions associated with a system that involve people, for example:

- performing manual monitoring operations,
- reviewing ISCM reports,
- following procedures, and
- making risk-based decisions.

Discussion. The Discussion attribute provides supplemental guidance to assessors on the assessment element, suggestions for what to look for with respect to specific objects, and sources of additional information/references. The discussion may provide additional detail about special situations or dependencies the assessor may need to consider.

Rationale for Level. Rationale for why the assessment element is assigned to a particular risk management level(s).

[19] [SP800-53A] discusses assurance in the assessment process.

Parent. Parent is the linkage to the previous process step assessment element that also addresses the same ISCM aspect or topic. The Define Step element does not have a parent assessment element.

Organizations are not expected to employ all assessment methods and objects contained within the assessment procedures. Rather, organizations have the flexibility to choose methods and objects and to determine the level of effort needed and the assurance required for an assessment, e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results.

Table 5 shows the format of the assessment element and its attributes as defined in the Assessment Element Catalog [Catalog].

Table 5 – Assessment Element Format

ID	Assessment Element Text	Level	Source	Assessment Procedure	Discussion	Rationale for Level	Parent
Identifier	*Assessment Element Text*	*Applicable risk management level*	*Authoritative source from which the assessment element is derived*	**ASSESSMENT OBJECTIVE** Determine if *objective* is met. **POTENTIAL ASSSESSMENT METHODS AND OBJECTS** Examine: *specifications* Interview: *personnel* Test: *mechanisms*	*Clarifying or supplemental information or additional guidance to the assessor.*	*Specifies why an assessment element is assigned to particular risk management levels.*	*Shows the linkage to a previous assessment process step*

Example of Assessment Element. Table 6 shows an example of an assessment element from the [Catalog].

Table 6 – Example Assessment Element

ID	Assessment Element Text	Level	Source	Assessment Procedure	Discussion	Rationale for Level	Parent
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	Level1	NIST SP 800-137	**ASSESSMENT OBJECTIVE** Determine if there is an ISCM program derived from the organization-wide ISCM strategy. **POTENTIAL ASSESSMENT METHODS AND OBJECTS** **Examine:** Organization-wide ISCM strategy; ISCM policy and procedure documentation; ISCM design documents; ISCM CONOPS. **Interview:** Level 1: SAISO; ISCM POC.	The ISCM program comprises the ISCM policies and procedures derived from the organization-wide ISCM strategy and includes the ISCM documents that guide ISCM implementation (e.g., ISCM technical architecture and ISCM CONOPS).	Level 1 is responsible for definition the ISCM program.	*The Define step has no parent element*

3.3.2 Use of Assessment Elements

Each assessment element in the Assessment Element [Catalog] applicable to the ISCM program assessment is acted upon (executed) by the assessor. The primary object in the assessment element is the assessment procedure, as defined in the previous section. The assessment objective is a re-statement of the assessment element about which the assessor makes a judgment of the degree to which a particular aspect of the ISCM program satisfies the element.

Each determination statement contained within an assessment objective of the assessment element (as shown in Table 6) produces, for example, one of the following judgments for the two-value judgment set (described in Sec. 2.2.6,): *Satisfied* or *Other than Satisfied*. A finding of *Satisfied* indicates that for the portion of the ISCM program being assessed the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for that assessment element has been met producing an acceptable result. For a finding of *Other than Satisfied*, the assessment provides for annotated reasons that explain the judgment, i.e., what portions of an assessment element prevent a *Satisfied* judgment. The reasons inform the organization of shortfalls in the ISCM program that may need to be addressed. A finding of *Other than Satisfied* may also indicate the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.

For assessment findings that are *Other than Satisfied*, organizations may choose to define subcategories of findings indicating the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects on organizations. Defining such subcategories can help to establish priorities for needed risk mitigation actions. Regardless of whether the organization defines subcategories, assessment results include sufficient information about shortfalls to indicate what further actions are required to completely satisfy the determination statement.

Figure 8 illustrates the use of the assessment element, using the example element presented in Table 6.

Use of Example Assessment Item Information

Steps 1 through 4 explain how the information fields of the example assessment element in Table 6 are used to arrive at a judgment about the example assessment element.

1. For the **Assessment Element** with **Identifier** 1-002**:**

> There is an ISCM program derived from the organization-wide ISCM strategy.

use the **POTENTIAL ASSESSMENT METHODS** on the **OBJECTS** as follows:

> 1. ***Examine:*** Organization-wide ISCM strategy; ISCM policy and procedure documentation; ISCM design documents; ISCM CONOPS.
>
> 2. ***Interview***: SAISO, ISCM POC

to obtain evidence to make a judgment about the ISCM **ASSESSMENT OBJECTIVE** below:

Determine if there is an ISCM program derived from the organization-wide ISCM strategy.

2. Use information relative to **Process Step** DEFINE and **Level** 1 from the Examine list and Interview List, as may be needed to help determine whether the ISCM **ASSESSMENT OBJECTIVE** is met.

3. Use **DISCUSSION:** "The ISCM program comprises the ISCM policies and procedures derived from the organization-wide ISCM strategy and includes the ISCM documents that guide ISCM implementation, (e.g., ISCM technical architecture and ISCM CONOPS)." to clarify wording or intent of the **Assessment Element**.

4. Make a judgment about how well assessment element is met (e.g., *Satisfied* or *Other than Satisfied*). Enter judgment into assessment tool or results repository. Annotate reasons for an *Other than Satisfied* judgment.

Figure 8 – Use of Example Assessment Item

Each assessment element is applied in a similar manner for each element in the [Catalog], and for each applicable organizational level. Results (judgments) for each assessment element are combined across multiple organization levels when the element applies to more than one level, as described in Sec. 2.2.9. The assessment elements offered with this publication in the [Catalog] generally do not inform the assessor how to make the actual judgment (e.g., *Satisfied* or *Other than Satisfied*) since criteria for satisfying an ISCM program assessment element may vary among systems, missions, and organizations. The assessment procedures lead the assessor to the judgment decision point, in accordance with the assessment objective, after applying the assessment methods to the suggested objects (the evidence). The assessment methodology defined here verifies the subject or topic of the assessment element (e.g., strategies, policies, procedures, the actions of following procedures, and ISCM reports) as specified in the assessment element text. Execution of each assessment element every time the ISCM program assessment is conducted, in the manner explained in Figure 8, helps ensure the repeatability of the ISCM program assessment process. [Catalog]

3.4 Limits on ISCM Program Assessment Elements

While the assessment [Catalog] includes the minimum set of ISCM program assessment elements, the organization, in conjunction with the assessor, may add assessment elements, or if the ISCM program assessment is limited by the number of ISCM process steps (as described in Sec. 2.3.2), assessment elements may be deleted or bypassed for a particular ISCM program assessment engagement. Section 3.5 explains tailoring the ISCM program assessment process.

The ISCM program assessment does not repeat or augment control assessments (conducted in accordance with [SP800-53A]), but verifies that the control assessments are conducted according to each assessment element's conditions (e.g., at specified frequencies).

3.5 Tailoring the ISCM Program Assessment Process

Tailoring is a cooperative process between the assessor and the evaluated organization that is undertaken to meet the organization's needs. The steps of the assessment process (as described in Sec. 3.2) and the assessment itself may be tailored. Tailoring helps adapt the assessment to unique organizational situations, such as a limited (incremental) assessment due to an immature ISCM program. Tailoring also helps facilitate adoption of the assessment across the entire organization where the sub-organizations may vary in degree of implementation or risk environment. Assessment elements and assessment procedures are flexible enough to be tailored to meet the organization's needs.

Tailoring of the ISCM program assessment may be needed based on an organization's specific implementation of the ISCM program. For example, for federal agencies, the assessment is tailored in a way that helps determine if organizational ISCM programs meet the federal ISCM requirements from the authoritative sources. ISCM program assessment tailoring is coordinated with the assessment organization to ensure the ISCM program assessment still verifies the required aspects of ISCM. All tailoring decisions are documented in the ISCM Program Assessment Plan.

Tailoring the ISCM Program Assessment Scope. At the start of the tailoring activity, decisions about the scope of the ISCM program assessment are made, such as which systems and system components (user endpoints, servers, networking components), are to be assessed with respect to the ISCM program implementation to provide credible assessment evidence. Tailoring the ISCM program assessment scope involves understanding the organization's ISCM requirements and constraints and modifying the assessment elements where necessary. For example, tailoring may be based on organizational structure, e.g., number and size of sub-organizations, or ISCM maturity, such as disparity in ISCM maturity among mission/business processes.

The scope of the assessment is determined by the organization's leadership. Assessment elements are tailored out of the catalog for a narrower scope, e.g., if the assessment is limited or incremental by number of ISCM process steps, as described in Sections 2.3.2 and 3.4. The assessment scope may also be limited to specific risk management levels, e.g., for a Level 1 only (organizational) scope, or a Level 3 only (system-level) scope.

Tailoring the Assessment Elements. Tailoring could result in modifications to fields/attributes for the assessment elements. Assessment elements may be reworded to incorporate concepts created by new technologies or techniques. The assessment element set may be tailored by creating additional elements or modifying by rewording as described in Sec. 2.2.7.

If the ISCM program assessment is assisted by a tool, tailoring of individual assessment elements may be problematic if the tool is not designed for modification of the assessment elements and their attributes.

3.6 Conclusion of the ISCM Program Assessment

The ISCM program assessment may provide the organization with recommendations to improve the ISCM program, to include areas of ISCM program design, implementation, operation, and governance. At the conclusion of an assessment, the assessors present a draft report, and after discussion with organization leadership, a final report that resolves any differences of opinion between the assessors and the organization is presented to the organization. See Sections 2.2.12 and 3.2.3 for more information on reporting ISCM program assessment results.

The ISCM program assessment effort may be intense and short lived, or it may be continuing at a lower level of effort. Organizational personnel may meet with the assessment team after conclusion of the assessment. Follow-on collaboration may also involve meetings with the organizational staff and assessment team.

Post-assessment engagement. The ISCM program assessment may be repeated at predetermined intervals, when certain milestones occur in the development of the organization's ISCM program, or when response actions from a previous assessment are completed to verify closure of the action. A follow-on assessment may be expanded in scope as the organization's ISCM program gains maturity.

References

[44 USC 3544] Title 44 U.S. Code, Sec. 3544, Definitions. 2006 ed. https://www.govinfo.gov/app/details/USCODE-2008-title44/USCODE-2008-title44-chap35-subchapIII-sec3544

[Catalog] National Institute of Standards and Technology (2020) *ISCM Assessment Procedures Catalog*. Available at https://csrc.nist.gov/publications/detail/sp/800-137a/draft

[CNSSI 4009] Committee for National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD) CNSS Instruction (CNSSI) 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CSF 1.1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

* E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. https://www.govinfo.gov/app/details/PLAW-107publ347

* Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

[FISMA2014] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

* Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat. 2946. https://www.govinfo.gov/app/details/PLAW-107publ347

[ISCMA Reqs] DHS Information Security Continuous Monitoring Assessment (ISCMA) Requirements.

[NISTIR8212] T.B.D. ([forthcoming]) Methodology for Assessing Information Security Continuous Monitoring Programs. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8212.

[OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular

A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[OMB M-11-33] Office of Management and Budget (2011) FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. (The White House, Washington, DC), OMB Memorandum M-04-04, September 14, 2011. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf

[OMB M-14-03] Office of Management and Budget (2013) Enhancing the Security of Federal Information and Information Systems. (The White House, Washington, DC), OMB Memorandum M-14-03, November 18, 2013. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2014/m-14-03.pdf

[SP800-37] 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

[SP800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP800-53] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[SP800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP800-137] 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

Appendix A Acronyms

Selected acronyms and abbreviations used in this publication are defined below.

AO	Authorizing Official
CISA	Cybersecurity Infrastructure Security Agency
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CSF	Cybersecurity Framework
FISMA	Federal Information Modernization Act
ISCM	Information Security Continuous Monitoring
NCCoE	National Cybersecurity Center of Excellence
NISTIR	NIST Interagency or Internal Report
RE(f)	Risk executive (function)
RMF	Risk Management Framework
OA	Ongoing Authorization
OMB	Office of Management and Budget
SAISO	Senior Agency Information Security Officer
SIEM	Security Information and Event Management
SISO	Senior Information Security Officer

Appendix B Glossary

aspect The subject or topic of an assessment element that is associated with a portion of the ISCM program under assessment.

assessment Depending on the context:

(a) A completed or planned action of evaluation of an organization, a mission or business process, or one or more systems and their environments; or
(b) The vehicle or template or worksheet that is used for each evaluation.

assessment element A specific ISCM concept to be evaluated in the context of a specific ISCM Process Step

assessment element attribute An item of information that is specifically applicable to an assessment element, such as the source for the assessment element or risk management level to which the element applies.

assessment element text A statement that should be true for a well-implemented ISCM program. This statement is the evaluation criteria part of an assessment element.

assessment method [SP800-53A] One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.

assessment objective [SP800-53A] A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement.

assessment procedure [SP800-53A] A set of assessment objectives and an associated set of assessment methods and assessment objects.

catalog The collection of all assessment elements

chain Two or more assessment elements that are linked by a common aspect of ISCM. Each chain has an assessment element in Program Step 1, DEFINE, called the *root*, which has no predecessor or parent element.

continuous monitoring [SP800-37] Maintaining ongoing awareness to support organizational risk decisions.

distributed self-assessment The least formal type of assessment, the element judgments are based on the evaluations by small groups that work in parallel.

element A statement about an ISCM concept that is true for a well-implemented ISCM program.

evaluation criteria The standards by which accomplishments of technical and operational effectiveness or suitability characteristics may be assessed. Evaluation criteria are a benchmark, standard, or factor against which conformance, performance, and suitability of a technical capability, activity, product, or plan is measured.

external assessment engagement Formal engagement led by a third-party assessment organization.

facilitated self-assessment Less formal than an internal assessment engagement, the element judgments determined by participant consensus on each element for a given level.

high value asset Those information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries.

internal assessment engagement Formal engagement led by a team within the organization that determines element judgments.

information security continuous monitoring (ISCM) program [SP800-137] A program established to collect information in accordance with organizational strategy, policies, procedures, and pre-established metrics, utilizing information readily available in part through implemented security controls.

information security continuous monitoring (ISCM) strategy A strategy that establishes an ISCM program.

judgment The association of one of the pre-configured evaluation choices with an element, from the context of a specific organizational level

judgment value Predefined values that represent the possible choices an assessor make in judging whether or how well information gathered satisfies an assessment element.

parent assessment element The assessment element in a prior process step from which the current element was derived.

practitioner experience A source of ISCM assessment elements based on the experience of individuals (practitioners) with experience in designing, implementing, and operating ISCM capabilities as well as security engineering experience.

process step A reference to one of the 6 steps in the ISCM process defined in NIST SP 800-137.

risk executive (function) [SP800-37] An individual or group within an organization that helps to ensure that (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Risk Management Framework (RMF) step
A reference to one of the 6 steps in the Risk Management Framework process defined in SP 800-37.

risk management level
One of three organizational levels defined in NIST SP 800-39: Level 1 (organizational level), Level 2 (mission/business process level), or Level 3(system level).

risk tolerance [SP800-137]
The level of risk an entity is willing to assume in order to achieve a potential desired result.

robustness
When applied to ISCM, a property that an ISCM capability is sufficiently accurate, complete, timely, and reliable to provide security status information to organization decision-makers to enable them to make risk-based decisions.

[CNSSI 4009]
The ability of an information assurance (IA) entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

security controls [SP800-53]
A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Senior Agency Information Security Officer (SAISO) [44 USC 3544]
Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. Note: Also known as senior information security officer (SISO) or chief information security officer (CISO).

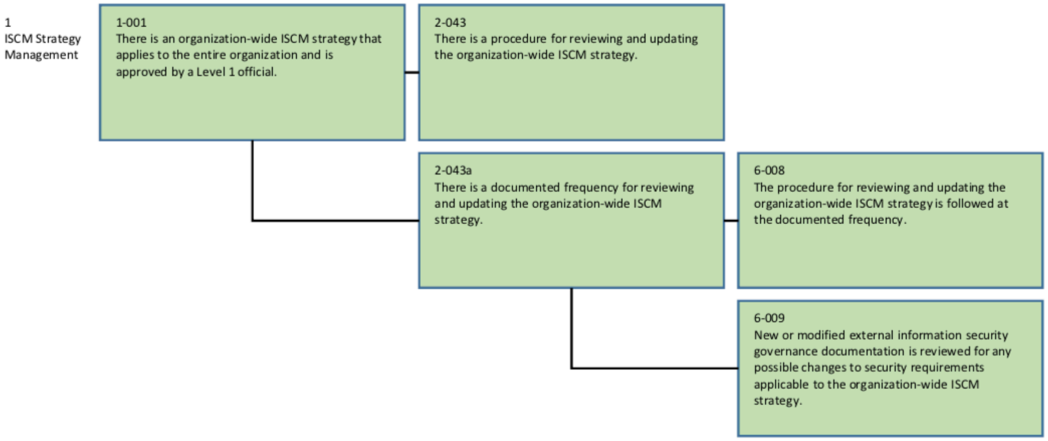
Senior Information Security Officer (SISO)
See Senior Agency Information Security Officer (SAISO)

System Security Officer (SSO) [SP800-37]
Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program

tailoring [SP800-53, adapted]
Similar in concept to tailoring baselines as described in SP 800-53, a cooperative process that modifies part of a set of assessment elements by (i) changing the scope of the assessment or risk management level; (ii) adding or eliminating assessment elements; or (iii) modifying the attributes of an assessment element.

Appendix C Traceability Chains

This Appendix presents the traceability chains (see Sec. 2.2.5) for the catalog of assessment elements provided with this publication. The string in the upper left of each element of the diagram provides unique identification of an individual assessment element.



1-001 There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.

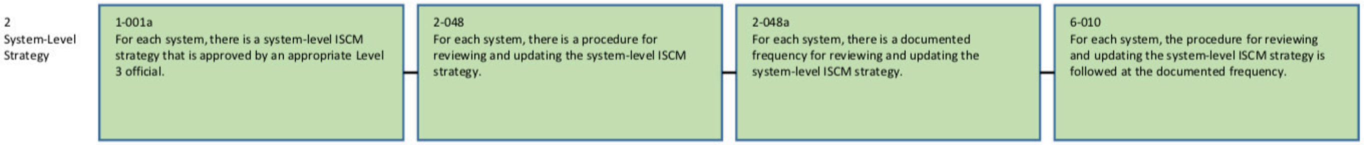
2-043 There is a procedure for reviewing and updating the organization-wide ISCM strategy.

2-043a There is a documented frequency for reviewing and updating the organization-wide ISCM strategy.

6-008 The procedure for reviewing and updating the organization-wide ISCM strategy is followed at the documented frequency.

6-009 New or modified external information security governance documentation is reviewed for any possible changes to security requirements applicable to the organization-wide ISCM strategy.

Figure 4 – ISCM Strategy Management Traceability Chain



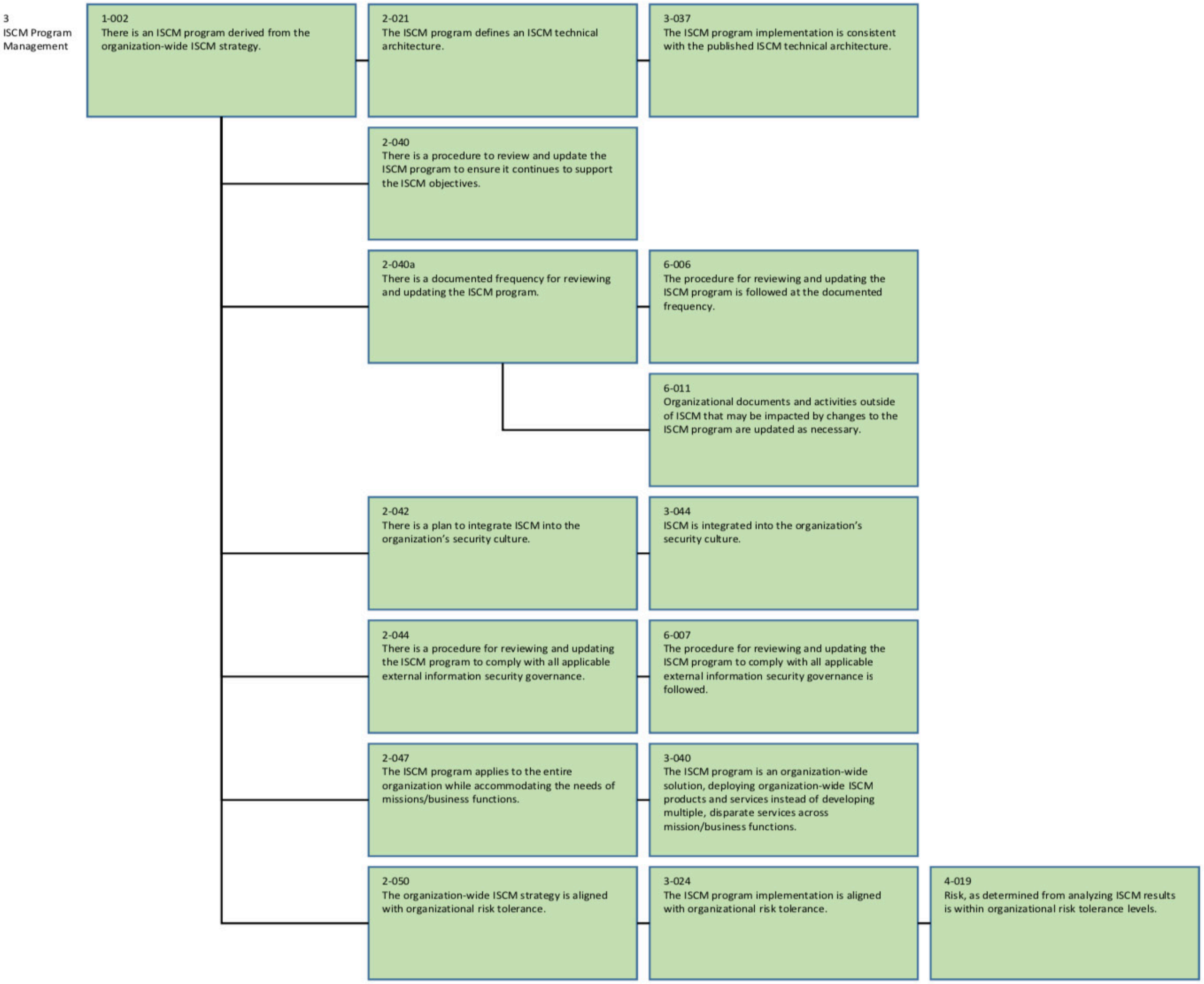
1-001a For each system, there is a system-level ISCM strategy that is approved by an appropriate Level 3 official.

2-048 For each system, there is a procedure for reviewing and updating the system-level ISCM strategy.

2-048a For each system, there is a documented frequency for reviewing and updating the system-level ISCM strategy.

6-010 For each system, the procedure for reviewing and updating the system-level ISCM strategy is followed at the documented frequency.

Figure 5 – System-level Strategy Traceability Chain



3
ISCM Program Management

1-002
There is an ISCM program derived from the organization-wide ISCM strategy.

2-021
The ISCM program defines an ISCM technical architecture.

3-037
The ISCM program implementation is consistent with the published ISCM technical architecture.

2-040
There is a procedure to review and update the ISCM program to ensure it continues to support the ISCM objectives.

2-040a
There is a documented frequency for reviewing and updating the ISCM program.

6-006
The procedure for reviewing and updating the ISCM program is followed at the documented frequency.

6-011
Organizational documents and activities outside of ISCM that may be impacted by changes to the ISCM program are updated as necessary.

2-042
There is a plan to integrate ISCM into the organization's security culture.

3-044
ISCM is integrated into the organization's security culture.

2-044
There is a procedure for reviewing and updating the ISCM program to comply with all applicable external information security governance.

6-007
The procedure for reviewing and updating the ISCM program to comply with all applicable external information security governance is followed.

2-047
The ISCM program applies to the entire organization while accommodating the needs of missions/business functions.

3-040
The ISCM program is an organization-wide solution, deploying organization-wide ISCM products and services instead of developing multiple, disparate services across mission/business functions.

2-050
The organization-wide ISCM strategy is aligned with organizational risk tolerance.

3-024
The ISCM program implementation is aligned with organizational risk tolerance.

4-019
Risk, as determined from analyzing ISCM results is within organizational risk tolerance levels.

Figure 6 – ISCM Program Management Traceability Chain

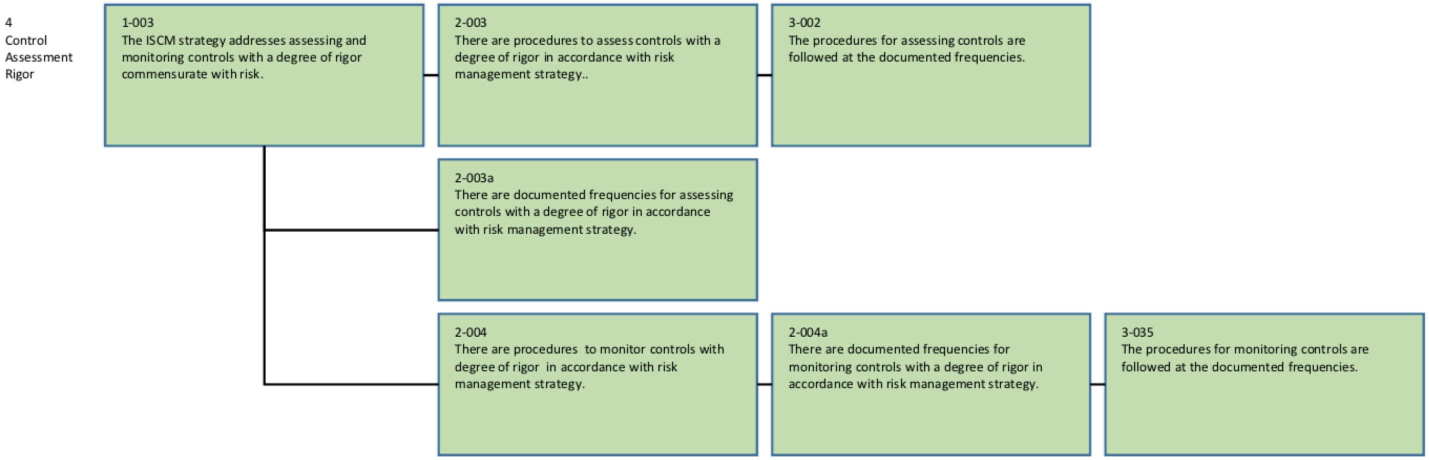

4 Control Assessment Rigor
1-003 The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.
2-003 There are procedures to assess controls with a degree of rigor in accordance with risk management strategy..
3-002 The procedures for assessing controls are followed at the documented frequencies.
2-003a There are documented frequencies for assessing controls with a degree of rigor in accordance with risk management strategy.
2-004 There are procedures to monitor controls with degree of rigor in accordance with risk management strategy.
2-004a There are documented frequencies for monitoring controls with a degree of rigor in accordance with risk management strategy.
3-035 The procedures for monitoring controls are followed at the documented frequencies.

Figure 7 – Control Assessment Rigor Traceability Chain

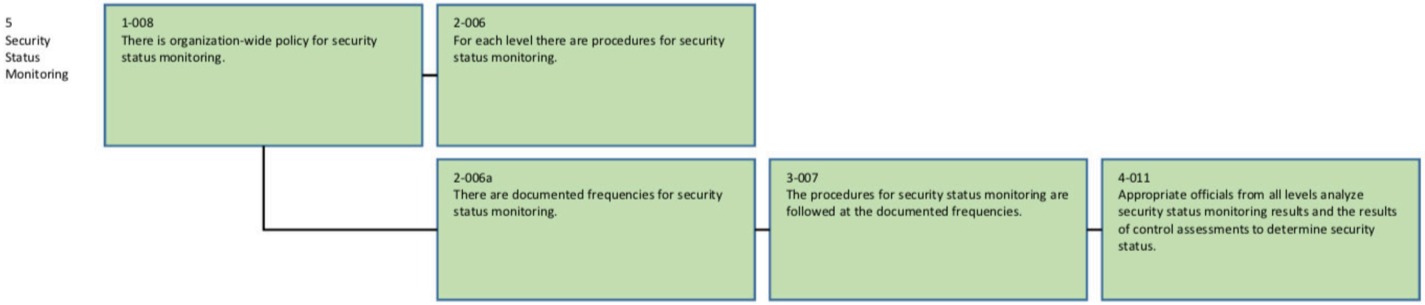

5 Security Status Monitoring
1-008 There is organization-wide policy for security status monitoring.
2-006 For each level there are procedures for security status monitoring.
2-006a There are documented frequencies for security status monitoring.
3-007 The procedures for security status monitoring are followed at the documented frequencies.
4-011 Appropriate officials from all levels analyze security status monitoring results and the results of control assessments to determine security status.

Figure 8 – Security Status Monitoring Traceability Chain

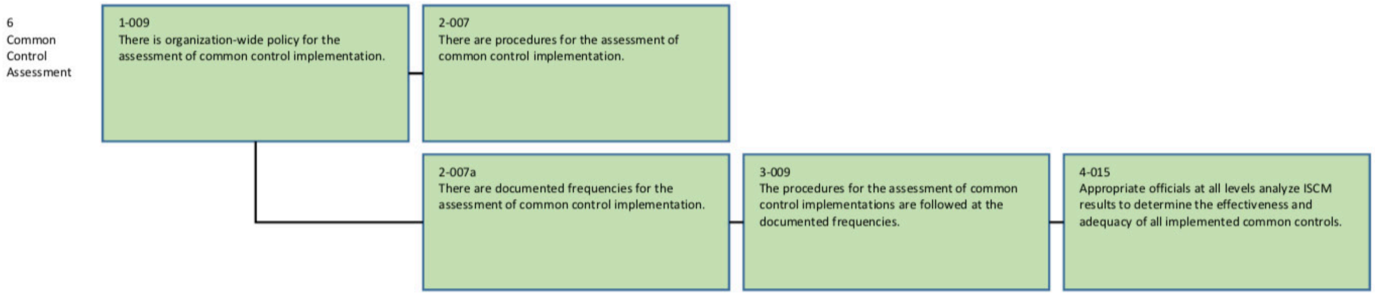

6
Common Control Assessment
1-009
There is organization-wide policy for the assessment of common control implementation.
2-007
There are procedures for the assessment of common control implementation.
2-007a
There are documented frequencies for the assessment of common control implementation.
3-009
The procedures for the assessment of common control implementations are followed at the documented frequencies.
4-015
Appropriate officials at all levels analyze ISCM results to determine the effectiveness and adequacy of all implemented common controls.

Figure 9 – Common Control Assessment Traceability Chain

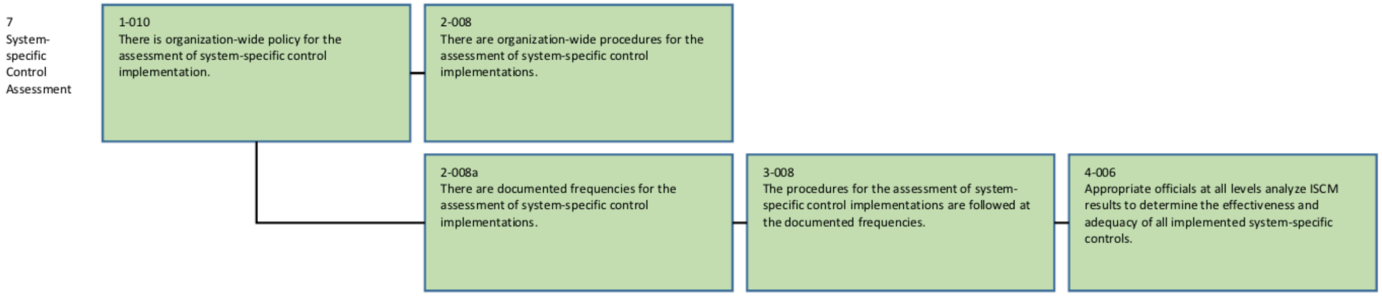

7
System-specific Control Assessment
1-010
There is organization-wide policy for the assessment of system-specific control implementation.
2-008
There are organization-wide procedures for the assessment of system-specific control implementations.
2-008a
There are documented frequencies for the assessment of system-specific control implementations.
3-008
The procedures for the assessment of system-specific control implementations are followed at the documented frequencies.
4-006
Appropriate officials at all levels analyze ISCM results to determine the effectiveness and adequacy of all implemented system-specific controls.

Figure 10 – System-specific Control Assessment Traceability Chain

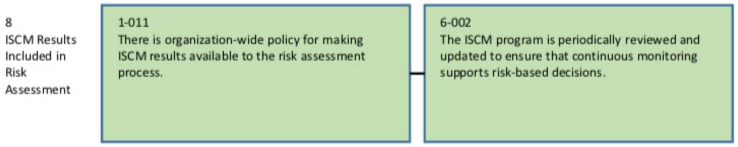
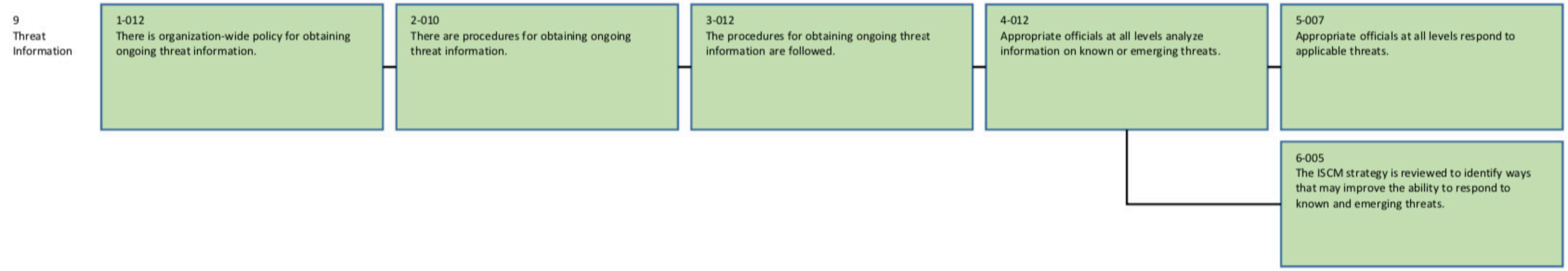

8
ISCM Results Included in Risk Assessment
1-011
There is organization-wide policy for making ISCM results available to the risk assessment process.
6-002
The ISCM program is periodically reviewed and updated to ensure that continuous monitoring supports risk-based decisions.

Figure 11 – ISCM Results Included in Risk Assessment Traceability Chain



9 Threat Information

1-012 There is organization-wide policy for obtaining ongoing threat information.

2-010 There are procedures for obtaining ongoing threat information.

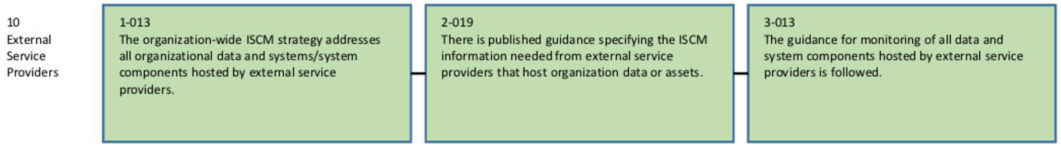
3-012 The procedures for obtaining ongoing threat information are followed.

4-012 Appropriate officials at all levels analyze information on known or emerging threats.

5-007 Appropriate officials at all levels respond to applicable threats.

6-005 The ISCM strategy is reviewed to identify ways that may improve the ability to respond to known and emerging threats.

Figure 12 – Threat Information Traceability Chain



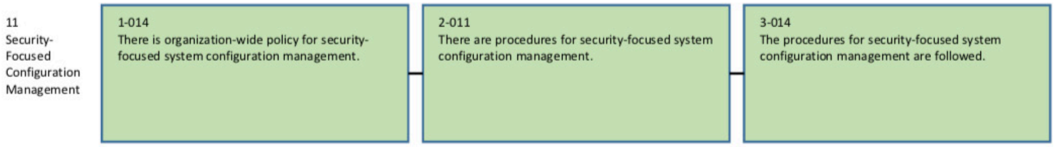
10 External Service Providers

1-013 The organization-wide ISCM strategy addresses all organizational data and systems/system components hosted by external service providers.

2-019 There is published guidance specifying the ISCM information needed from external service providers that host organization data or assets.

3-013 The guidance for monitoring of all data and system components hosted by external service providers is followed.

Figure 13 – External Service Providers Traceability Chain



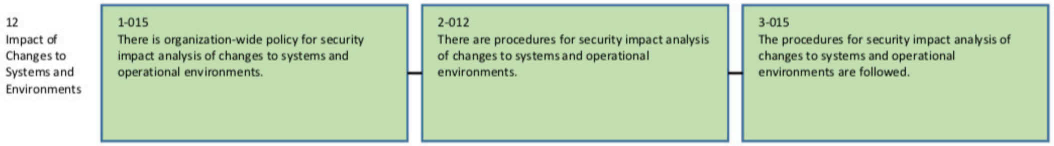
11 Security-Focused Configuration Management

1-014 There is organization-wide policy for security-focused system configuration management.

2-011 There are procedures for security-focused system configuration management.

3-014 The procedures for security-focused system configuration management are followed.

Figure 14 – Security-focused Configuration Management Traceability Chain



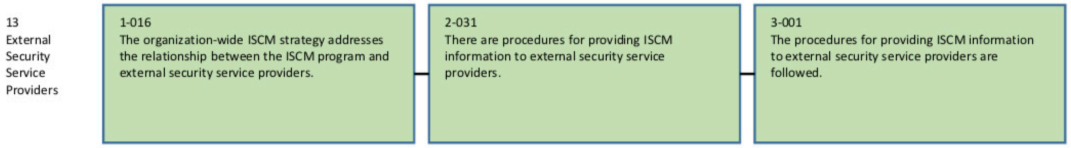
12
Impact of Changes to Systems and Environments

1-015
There is organization-wide policy for security impact analysis of changes to systems and operational environments.

2-012
There are procedures for security impact analysis of changes to systems and operational environments.

3-015
The procedures for security impact analysis of changes to systems and operational environments are followed.

Figure 15 – Impact of Changes to Systems and Environments Traceability Chain



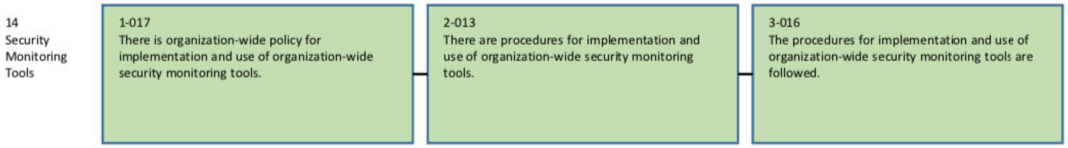
13
External Security Service Providers

1-016
The organization-wide ISCM strategy addresses the relationship between the ISCM program and external security service providers.

2-031
There are procedures for providing ISCM information to external security service providers.

3-001
The procedures for providing ISCM information to external security service providers are followed.

Figure 16 – External Security Service Providers Traceability Chain



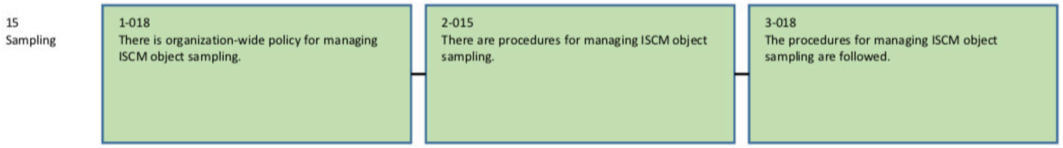
14
Security Monitoring Tools

1-017
There is organization-wide policy for implementation and use of organization-wide security monitoring tools.

2-013
There are procedures for implementation and use of organization-wide security monitoring tools.

3-016
The procedures for implementation and use of organization-wide security monitoring tools are followed.

Figure 17 – Security Monitoring Tools Traceability Chain



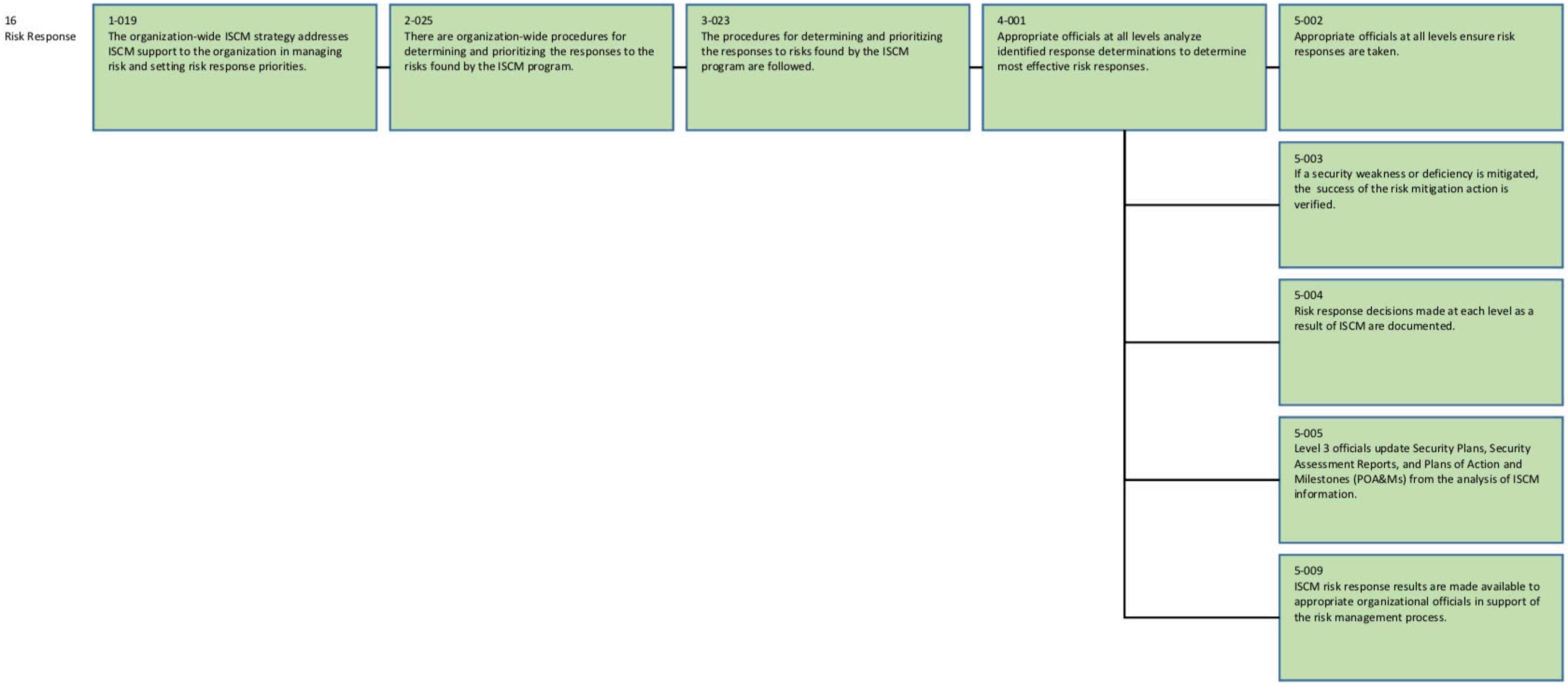
15
Sampling

1-018
There is organization-wide policy for managing ISCM object sampling.

2-015
There are procedures for managing ISCM object sampling.

3-018
The procedures for managing ISCM object sampling are followed.

Figure 18 – Sampling Traceability Chain



16
Risk Response

1-019
The organization-wide ISCM strategy addresses ISCM support to the organization in managing risk and setting risk response priorities.

2-025
There are organization-wide procedures for determining and prioritizing the responses to the risks found by the ISCM program.

3-023
The procedures for determining and prioritizing the responses to risks found by the ISCM program are followed.

4-001
Appropriate officials at all levels analyze identified response determinations to determine most effective risk responses.

5-002
Appropriate officials at all levels ensure risk responses are taken.

5-003
If a security weakness or deficiency is mitigated, the success of the risk mitigation action is verified.

5-004
Risk response decisions made at each level as a result of ISCM are documented.

5-005
Level 3 officials update Security Plans, Security Assessment Reports, and Plans of Action and Milestones (POA&Ms) from the analysis of ISCM information.

5-009
ISCM risk response results are made available to appropriate organizational officials in support of the risk management process.

Figure 19 – Risk Response Traceability Chain

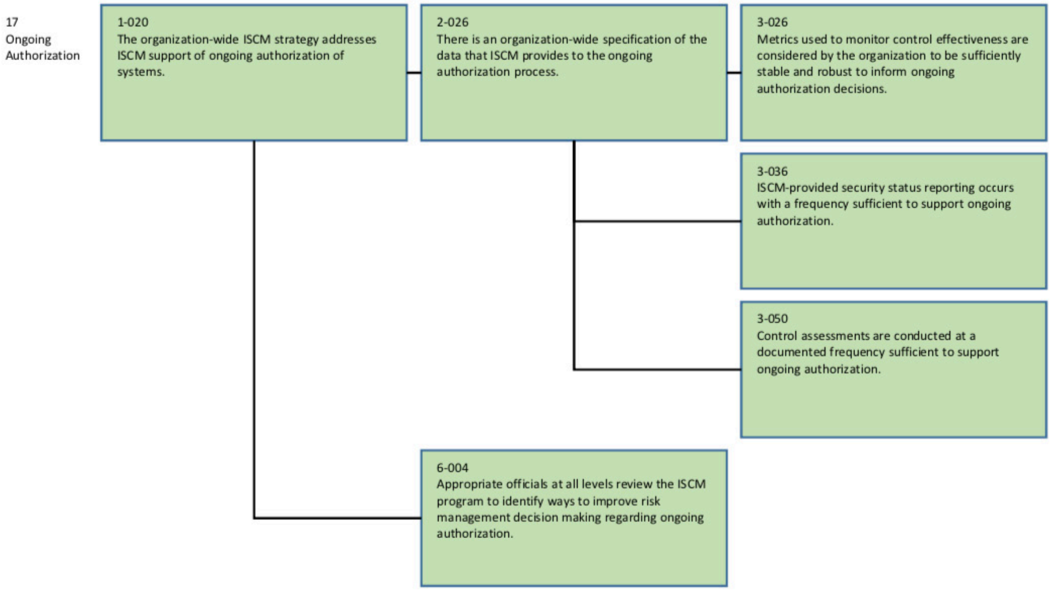

17
Ongoing
Authorization
1-020
The organization-wide ISCM strategy addresses ISCM support of ongoing authorization of systems.
2-026
There is an organization-wide specification of the data that ISCM provides to the ongoing authorization process.
3-026
Metrics used to monitor control effectiveness are considered by the organization to be sufficiently stable and robust to inform ongoing authorization decisions.
3-036
ISCM-provided security status reporting occurs with a frequency sufficient to support ongoing authorization.
3-050
Control assessments are conducted at a documented frequency sufficient to support ongoing authorization.
6-004
Appropriate officials at all levels review the ISCM program to identify ways to improve risk management decision making regarding ongoing authorization.

Figure 20 – Ongoing Authorization Traceability Chain

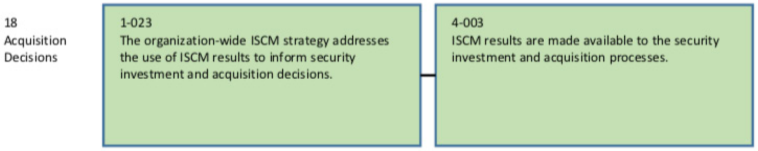
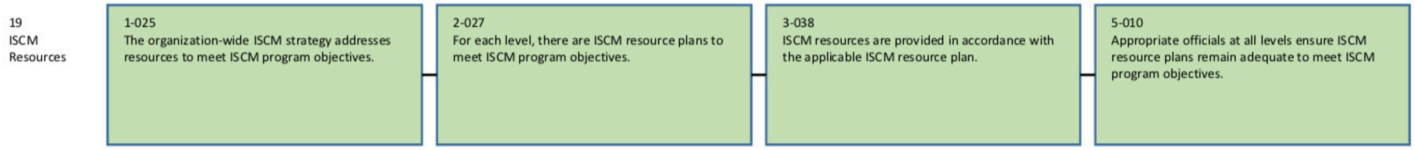

18
Acquisition
Decisions
1-023
The organization-wide ISCM strategy addresses the use of ISCM results to inform security investment and acquisition decisions.
4-003
ISCM results are made available to the security investment and acquisition processes.

Figure 21 – Acquisition Decisions Traceability Chain



19
ISCM
Resources

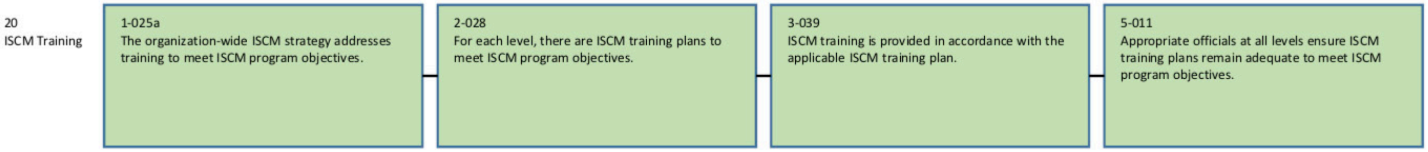
1-025
The organization-wide ISCM strategy addresses resources to meet ISCM program objectives.

2-027
For each level, there are ISCM resource plans to meet ISCM program objectives.

3-038
ISCM resources are provided in accordance with the applicable ISCM resource plan.

5-010
Appropriate officials at all levels ensure ISCM resource plans remain adequate to meet ISCM program objectives.

Figure 22 – ISCM Resources Traceability Chain



20
ISCM Training

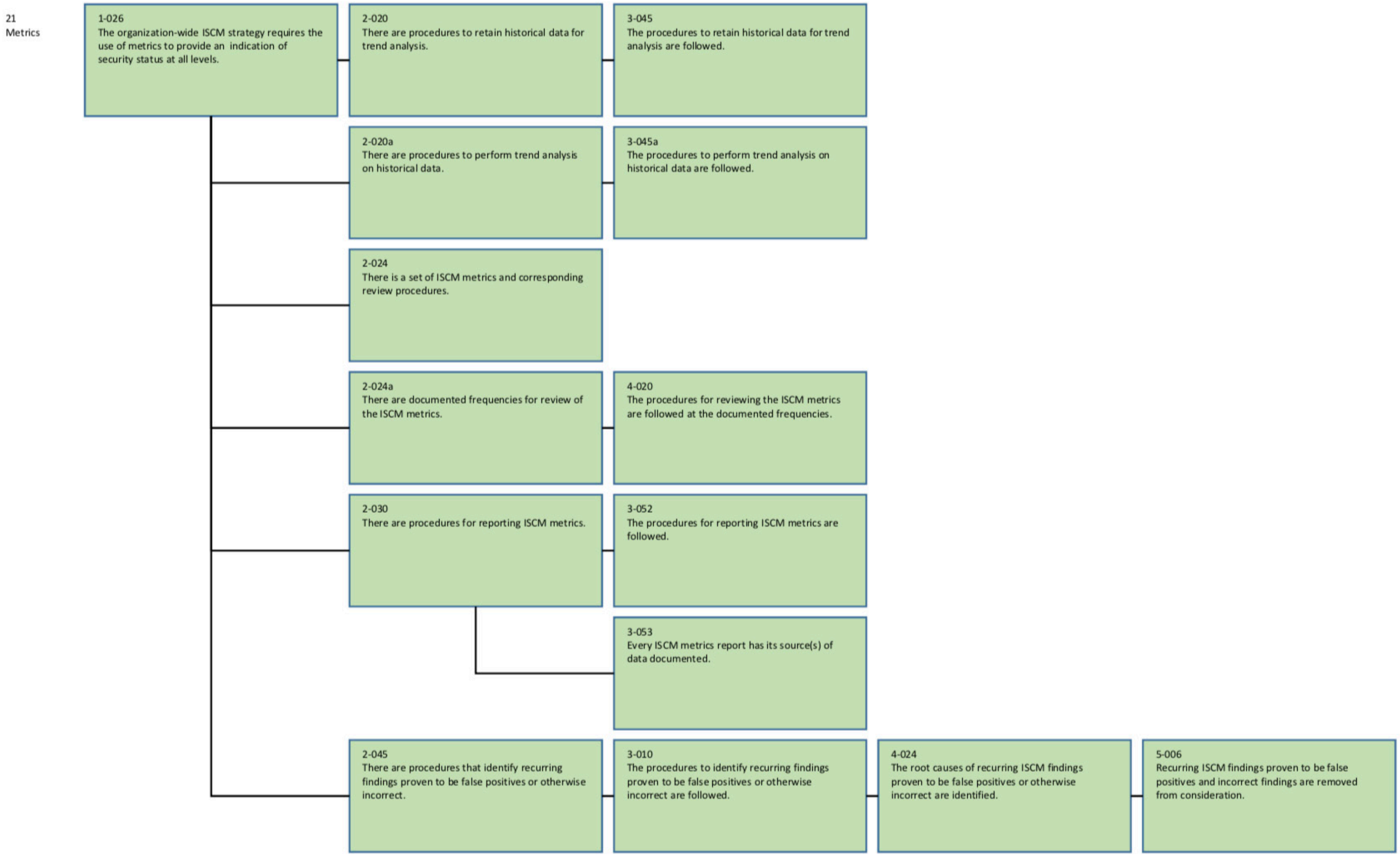
1-025a
The organization-wide ISCM strategy addresses training to meet ISCM program objectives.

2-028
For each level, there are ISCM training plans to meet ISCM program objectives.

3-039
ISCM training is provided in accordance with the applicable ISCM training plan.

5-011
Appropriate officials at all levels ensure ISCM training plans remain adequate to meet ISCM program objectives.

Figure 23 – ISCM Training Traceability Chain



21
Metrics

1-026
The organization-wide ISCM strategy requires the use of metrics to provide an indication of security status at all levels.

2-020
There are procedures to retain historical data for trend analysis.

3-045
The procedures to retain historical data for trend analysis are followed.

2-020a
There are procedures to perform trend analysis on historical data.

3-045a
The procedures to perform trend analysis on historical data are followed.

2-024
There is a set of ISCM metrics and corresponding review procedures.

2-024a
There are documented frequencies for review of the ISCM metrics.

4-020
The procedures for reviewing the ISCM metrics are followed at the documented frequencies.

2-030
There are procedures for reporting ISCM metrics.

3-052
The procedures for reporting ISCM metrics are followed.

3-053
Every ISCM metrics report has its source(s) of data documented.

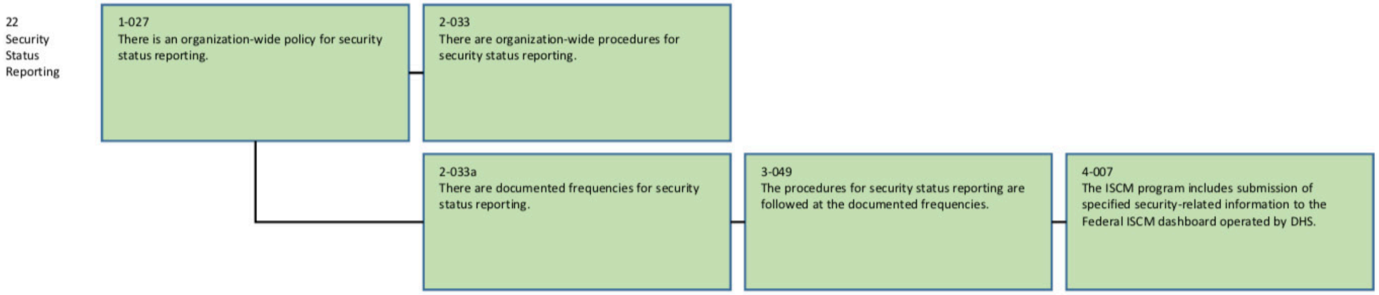
2-045
There are procedures that identify recurring findings proven to be false positives or otherwise incorrect.

3-010
The procedures to identify recurring findings proven to be false positives or otherwise incorrect are followed.

4-024
The root causes of recurring ISCM findings proven to be false positives or otherwise incorrect are identified.

5-006
Recurring ISCM findings proven to be false positives and incorrect findings are removed from consideration.

Figure 24 – Metrics Traceability Chain



22
Security Status Reporting

1-027
There is an organization-wide policy for security status reporting.

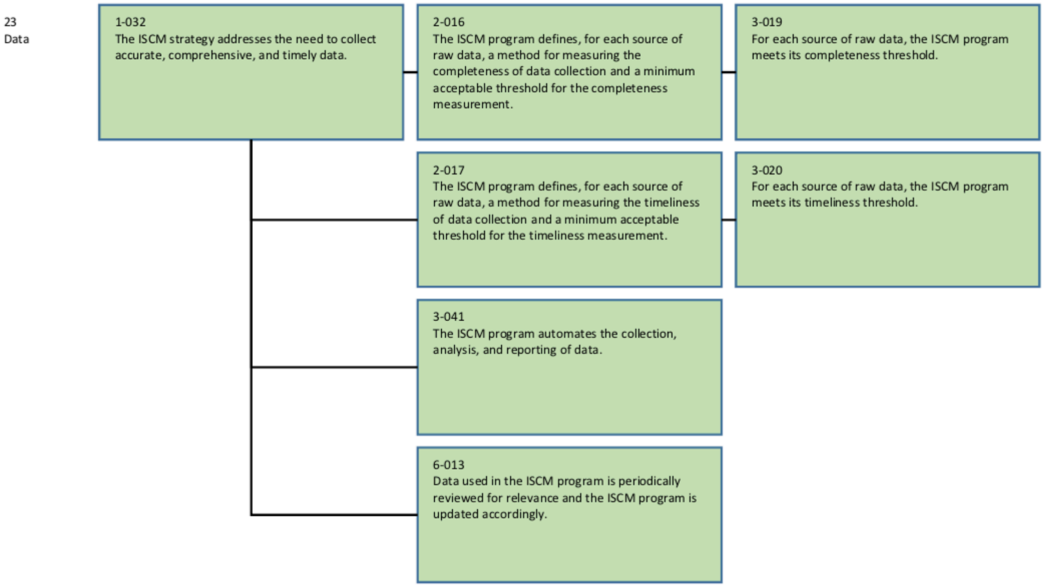
2-033
There are organization-wide procedures for security status reporting.

2-033a
There are documented frequencies for security status reporting.

3-049
The procedures for security status reporting are followed at the documented frequencies.

4-007
The ISCM program includes submission of specified security-related information to the Federal ISCM dashboard operated by DHS.

Figure 25 – Security Status Monitoring Traceability Chain



23
Data

1-032
The ISCM strategy addresses the need to collect accurate, comprehensive, and timely data.

2-016
The ISCM program defines, for each source of raw data, a method for measuring the completeness of data collection and a minimum acceptable threshold for the completeness measurement.

3-019
For each source of raw data, the ISCM program meets its completeness threshold.

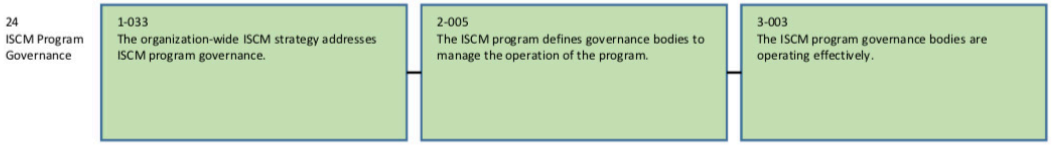
2-017
The ISCM program defines, for each source of raw data, a method for measuring the timeliness of data collection and a minimum acceptable threshold for the timeliness measurement.

3-020
For each source of raw data, the ISCM program meets its timeliness threshold.

3-041
The ISCM program automates the collection, analysis, and reporting of data.

6-013
Data used in the ISCM program is periodically reviewed for relevance and the ISCM program is updated accordingly.

Figure 26 – Data Traceability Chain



24
ISCM Program Governance

1-033
The organization-wide ISCM strategy addresses ISCM program governance.

2-005
The ISCM program defines governance bodies to manage the operation of the program.

3-003
The ISCM program governance bodies are operating effectively.

Figure 27 – ISCM Program Governance Traceability Chain