DRAFT NISTIR 8212

ISCMA: An Information Security Continuous Monitoring Program Assessment

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8212-draft

National Institute of
Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8212

ISCMA: An Information Security Continuous Monitoring Program Assessment

Kelley Dempsey
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

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

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8212-draft

October 2020

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

National Institute of Standards and Technology Interagency or Internal Report 8212
73 pages (October 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8212-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: *October 1, 2020* through *November 13, 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.

Abstract

This publication describes an example methodology for assessing an organization's Information Security Continuous Monitoring (ISCM) program. It was developed directly from NIST guidance and is applicable to any organization, public or private. It can be used as documented or as the starting point for a different methodology. Included with the methodology is a reference implementation that is directly usable for conducting an ISCM assessment.

Keywords

assessment; continuous monitoring; information security continuous monitoring; information security continuous monitoring assessment; ISCM; ISCMA; ISCMAx.

Acknowledgments

The authors wish to thank the numerous reviewers, and in particular Mr. Robert L. Heinemann, Jr. of the MITRE Corporation, for their insightful feedback. The authors also gratefully acknowledge the contribution of the assessors at the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency and who piloted the initial version of the methodology described in this report. In addition, a special note of thanks goes to Jim Foti, Lorin Smith, Isabel Van Wyk, and the NIST web team for their outstanding administrative support.

Audience

The audience for this report consists of organizations desiring to establish or improve their ISCM programs. This includes federal, state, local, and tribal agencies, as well as private non-government organizations.

Note to Reviewers

The ISCMAx tool, available from the link at: https://csrc.nist.gov/publications/detail/nistir/8212/draft in "Supplemental Content" is intended for use as companion tool for conducting ISCM Program Assessment Reviews.

Trademark Information

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

National Institute of Standards and Technology Interagency Report (NISTIR) 8212 provides an operational approach to the assessment of an organization's Information Security Continuous Monitoring (ISCM) program.[1] The ISCM assessment (ISCMA) approach is consistent with ISCM Program Assessment as described in NIST SP 800-137A [SP800-137A], Assessing Information Security Continuous Monitoring Programs: Developing an ISCM Program Assessment.

Included with the ISCMA approach in this report is ISCMAx [ISCMAx], a free, publicly available working implementation of ISCMA that can be tailored to fit the needs of the organization.

ISCMAx is suited for self-assessment by organizations of any size or complexity. Organizations choose the desired breadth and depth of the assessment. Breadth options are provided for organizations ranging from those that already have functioning ISCM programs to those that are just starting. Depth options allow organizations to focus on the more critical aspects of the program followed by details and nuances.

The ISCMA is designed around participation by personnel from the following risk management levels[2] and associated ISCM responsibilities:

- Level 1 personnel are responsible for the organization-wide ISCM strategy, policies, procedures, and implementation.
- Level 2 personnel are responsible for the ISCM strategy, policies, procedures, and implementation for specific mission/business functions.
- Level 3 personnel are responsible for ISCM strategy, policies, procedures, and implementation for individual information systems.

At each risk management level, an ISCMA unique to that level is conducted. Judgments are made about assessment elements, which are statements that should be true for a well-implemented ISCM program. Under ISCMA, an assessment with the maximum breadth and depth consists of 128 assessment elements. The results for each risk management level are then merged into a single overall result.

The ISCMA process proceeds according to the following five steps:

[1] ISCM is defined in NIST Special Publication (SP) 800-137 [SP800-137], *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[2] Risk management levels are described in NIST SP 800-39 [SP800-39], *Managing Information Security Risk: Organization, Mission, and Information System View.*

1. Plan the approach
2. Evaluate the elements
3. Score the judgments
4. Analyze the results
5. Formulate actions

Part of step 1, "plan the approach," is to determine how to organize the selected participants at each risk management level. For example, all participants from Level 2 could conduct a single ISCMA as a group with judgments made by consensus. Alternatively, participants from each mission/business process could conduct individual assessments in parallel and allow [ISCMAx] to assemble and merge those assessments. In the latter case, the most common judgment of all the individual assessments is the overall judgment for a risk management level.

ISCMAx produces a detailed scorecard and associated graphical output. It also automatically reports conditions that may warrant further analysis, such as:

- Elements where the overall organizational judgment is weakest
- Elements where different risk management levels have widely divergent judgments

The ISCMAx tool is a Microsoft Excel application and can be used immediately in the Windows operating system without involving support groups. This report includes complete instructions for both using ISCMAx as provided and for tailoring it, if desired.

Table of Contents

Executive Summary ... vii

1 Introduction ... 1

1.1 Purpose and Scope ... 1
1.2 Target Audience ... 1
1.3 Relationship to Other NIST Documents ... 1
1.4 Organization of this Report ... 2

2 ISCMA: An ISCM Program Assessment ... 2

2.1 Design Principles ... 3
2.2 Engagement Types ... 3
2.3 Assessment Elements ... 4
2.4 Incremental Assessments ... 5
2.5 Risk Management Levels ... 6
2.6 Judgments ... 7
2.7 Reporting Views ... 7
2.7.1 Section View ... 8
2.7.2 Perspective View ... 10
2.7.3 Process Step View ... 10
2.7.4 CSF Category View ... 10
2.8 The ISCMA Process ... 10
2.8.1 Plan the Approach ... 11
2.8.2 Evaluate the Elements ... 14
2.8.3 Score the Judgments ... 16
2.8.4 Analyze the Results ... 17
2.8.5 Formulate Actions ... 18
2.9 The Use of Consensus ... 18

3 ISCMAx: The ISCMA Methodology Assessment Tool ... 19

3.1 ISCMAx and Excel ... 19
3.2 Obtaining ISCMAx ... 20
3.3 Overview of ISCMAx Processing ... 20
3.4 Starting ISCMAx ... 20

3.5 Assessment Parameters 22
3.6 Element Evaluation 23
3.6.1 Judgment Selection 25
3.6.2 Element-Level Judgment Assistance 25
3.7 Scoring and Partial Results 26
3.8 Action Buttons 27
3.8.1 Restart Assessment 27
3.8.2 Merge Assessments 28
3.8.3 Export Data 28
3.8.4 Tailor Assessment 28
3.9 Deploying the Workbook 28
3.10 Additional Underlying Worksheets 29
4 The Master Assessment Workbook 29
4.1 The Merge Process 29
4.2 ScoreSummary Worksheet 32
4.3 Differences Worksheet 35
4.4 Messages Worksheet 36
4.5 Observations Worksheet 36
4.6 Single Judgment Worksheets 37
4.7 Notes and Recommendations Worksheet 38
4.8 Relative Judgment Numbers 38
4.9 MasterAssessment Worksheet 38
4.10 Level Worksheets 39
4.11 Chains Worksheet 41
4.12 JudgmentTable Worksheet 42
5 Tailoring 43
5.1 Tailoring the Elements 43
5.2 Tailoring Views 46
5.3 Tailoring Judgments 47
5.3.1 Judgment Labels 48
5.3.2 Intra-Level Judgment Conflict Resolution 48
5.3.3 The Judgment Combination Table 49

5.3.4 Summary of Judgment Tailoring Actions 50
5.4 Tailoring Scoring 51
5.5 Miscellaneous Tailoring 53
5.5.1 Tailoring the Instructions 53
5.5.2 Tailoring Miscellaneous Behavior Configurations 53
5.6 Example of Tailoring Judgments and Scoring 54
5.7 The ISCMAx Version Identifier 55
5.8 The Future of ISCMAx 56

List of Appendices

Appendix A— Glossary 57

Appendix B— References 59

List of Figures

Figure 1 – NIST ISCM Document Relationship 2
Figure 2 - ISCMA Process 11
Figure 3 - ISCMA *Plan the Approach* 11
Figure 4 - ISCMA *Evaluate the Elements* 14
Figure 5 - ISCMA *Score the Judgments* 16
Figure 6 - Inter-Level Consolidation (Recommended Judgments) 16
Figure 7 - Inter-Level Consolidation (Alternate Judgments) 17
Figure 8 - ISCMA *Analyze the Results* 17
Figure 9 - ISCMA *Formulate Actions* 18
Figure 10 - ISCMA Partially Automated Steps 20
Figure 11 - Required References 21
Figure 12 - TitlePage Worksheet 21
Figure 13 - Assessment Worksheet (Recommended Judgments) 22
Figure 14 - Assessment Worksheet (Alternate Judgments) 22
Figure 15 - Specifying a Detailed Level 1 Assessment of the Full ISCM Program 23
Figure 16 - Assessment Parameter Display 23
Figure 17 - Element Evaluation Screen (Recommended Judgments) 24

Figure 18 - Element Evaluation Screen (Alternate Judgments) 25

Figure 19 - Notes/Help Icon 26

Figure 20 – Element-Level Judgment Assistance 26

Figure 21 - Score Summary 27

Figure 22 - Action Buttons 27

Figure 23 - Master Assessment Worksheet List 31

Figure 24 - Merge Process 32

Figure 25 - ScoreSummary Worksheet 33

Figure 26 – Score Summary Bar 34

Figure 27 - View Scorecard 35

Figure 28 - Differences Worksheet 35

Figure 29 - Messages Worksheet 36

Figure 30 - Observation Worksheet 36

Figure 31 - Other Than Satisfied Worksheet (Recommended Judgments) 37

Figure 32 - CompletelyFalse Worksheet (Alternate Judgments) 37

Figure 33 - MasterAssessment Worksheet (Recommended Judgments) 39

Figure 34 - MasterAssessment Worksheet (Alternate Judgments) 39

Figure 35 - Level3 Worksheet (Recommended Judgments) 40

Figure 36 – Level1 Worksheet (Alternate Judgments) 41

Figure 37 - Chain (Recommended Judgments) 42

Figure 38 - Chain (Alternate Judgments) 42

Figure 39 - Judgment Combination Table (Recommended Judgments) 43

Figure 40 - Judgment Combination Table (Alternate Judgments) 43

Figure 41 - Judgment Configuration Parameters (Recommended Judgments) 48

Figure 42 - Judgment Configuration Parameters (Alternate Judgments) 48

Figure 43 - Intra-Level Judgment Conflict Resolution Setting 49

Figure 44 - Judgment Combination Table Details (Recommended Judgments) 49

Figure 45 - Judgment Combination Table Details (Alternate Judgments) 50

Figure 46 - Judgments and Scoring Tailoring (Recommended Judgments) 52

Figure 47 - Judgment and Scoring Tailoring (Alternate Judgments) 52

Figure 48 - Configuring a 1-10 Scale 54

Figure 49 - Using a 1-10 Scale 55

Figure 50 - Modifying the ISCMAx Version Identifier 56

List of Tables

Table 1 - Key ISCMA Design Principles 3
Table 2 - Assessment Engagement Types 3
Table 3 – Assessment Element Information Fields 5
Table 4 – Section View 8
Table 5 – Perspective View 10
Table 6 – Number of Elements by Process Step 12
Table 7 – Number of Elements by Level Combination 12
Table 8 - Total Judgments by Level 13
Table 9 - Underlying Worksheets 29
Table 10 - Master Assessment Worksheets 31
Table 11 - Elements Worksheet 44
Table 12 – Tailoring Actions for the Element Worksheet 45
Table 13 - ISCMA View Tailoring Actions 47
Table 14 - Judgment Tailoring Actions 51
Table 15 - ISCMA Scoring Tailoring Actions 53
Table 16 - Miscellaneous Behavior Configuration 54

1 Introduction

1.1 Purpose and Scope

The purpose of National Institute of Standards (NIST) Interagency Report (IR) 8212 is to provide an operational approach to the assessment of an organization's Information Security Continuous Monitoring (ISCM) program.

A robust ISCM program integrates continual improvements in all aspects of an ISCM program to include people, processes, technology, and data. To help ensure that all aspects of the ISCM program continue to be effective and are operating as intended, each aspect of the ISCM program is assessed periodically, much like security controls. This report describes an ISCM program assessment (ISCMA) that is based on NIST guidance and is adaptable to specific organizational requirements. In addition, included with this report is [ISCMAx]—a free, publicly available implementation of ISCMA.

1.2 Target Audience

The target audience for this report consists of organizations that wish to establish or improve their ISCM programs. This includes federal, state, local, and tribal agencies, as well as private non-governmental organizations.

1.3 Relationship to Other NIST Documents

This report is based on the following NIST guidance documents:

- NIST SP 800-137 [SP800-137] describes the desirable properties of an ISCM program and the process for establishing an ISCM program in an organization.
- NIST SP 800-137A [SP800-137A] describes the desirable properties of an ISCM program assessment methodology and the process for assessing the effectiveness of an ISCM program in an organization. The assessment methodology described in SP 800-137A has been followed in this report and implemented in the [ISCMAx] companion tool.

The relationship between the guidance documents, this report, and the accompanying tool is represented in Figure 1.

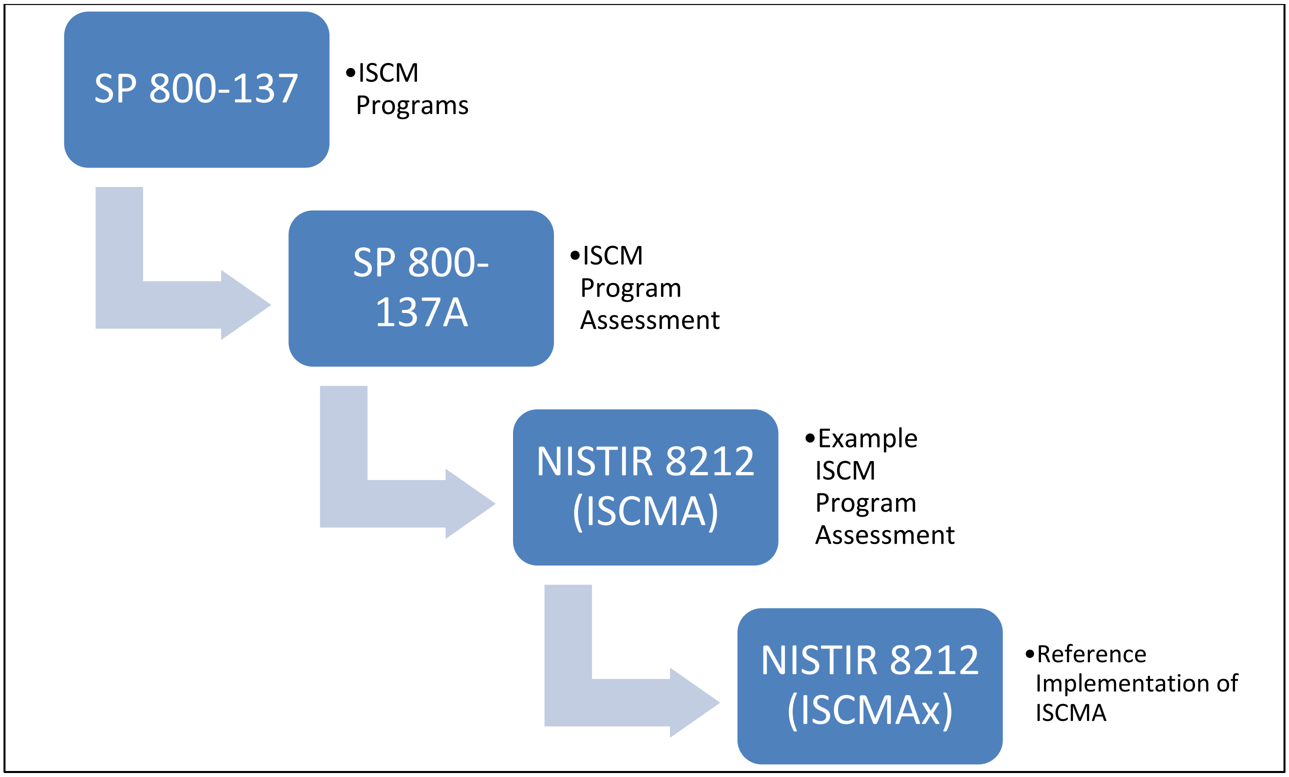


Figure 1 – NIST ISCM Document Relationship

1.4 Organization of this Report

Section 2 provides a summary of the key underpinnings of the ISCMA methodology. Section 3 describes the ISCMA Tool, [ISCMAx], that is provided in a separate companion file as a reference implementation of ISCMA. Section 4 describes the overall assessment report that results from using ISCMAx at all risk management levels. Section 5 discusses ways in which both the ISCMA and ISCMAx can be tailored to better meet specific organizational requirements.

This report discusses a set of *Assessment Elements*, which form the foundation of ISCMA, but it does not include a complete list. All assessment elements can be found in the ISCMAx tool, as well as in the assessment element catalog [Catalog] that accompanies [SP800-137A].

2 ISCMA: An ISCM Program Assessment

ISCMA is a specific example of an ISCM program assessment based on the guidelines described in [SP800-137A], which outlines the decisions that are made in establishing an ISCM program assessment, and the assessment template provided by the ISCMA element [Catalog], which establishes the ISCMA elements and their attributes. Organizations may make different assessment decisions in accordance with their individual requirements.

2.1 Design Principles

ISCMA follows [SP800-137A] closely. Table 1 lists the design principles of ISCMA and describes the ISCMA features that support them.

Table 1 - Key ISCMA Design Principles

Design Principle	ISCMA/ISCMAx Implementation
Capable of adapting as organizational ISCM programs mature	Choice of breadth (Section 2.4) and depth (Section 2.8.1)
Adaptable to the structure of the organization being assessed (e.g., centralized vs. decentralized)	Distributed assessment support (Section 2.2)
Applicable to any size organization	Distributed assessment support (Section 2.2)
Produce actionable results	Recommendation support (Sections 4.6 and 4.7)
Allow more granular reporting choices within the primary judgments	Judgment system (Section 2.6)

2.2 Engagement Types

ISCMA supports the engagement types described in [SP800-137A] and shown in Table 2.

Table 2 - Assessment Engagement Types

Engagement Type	Description
External Assessment Engagement	Formal engagement facilitated by a third-party assessment organization that makes the judgments about each element. An external assessment is conducted by trained staff and provides the greatest objectivity.
Internal Assessment Engagement	Formal engagement, facilitated by a team within the organization that makes the judgments about each element.
Facilitated Self-Assessment	A less formal engagement, facilitated by a team within the organization that records element judgments based on participant consensus.
Distributed Self-Assessment	The least formal type of assessment, led by an internal team that coordinates the distribution of judgment-making to small groups that work in parallel. A group can consist of as few as one person. The individual results are then assembled, combined by algorithm, analyzed, and presented to the organization for action.

Support for the distributed self-assessment engagement type drives much of the design of ISCMA.

2.3 Assessment Elements

The primary data construct of the ISCMA methodology is an *assessment element,* usually referred to in this report simply as an *element*. Each element is a statement about an ISCM program that is expected to be true for a well-designed, well-implemented program.

ISCMA implements the complete set of elements defined in [SP800-137A]. The elements were identified in SP 800-137A as being representative of the fundamental concepts of ISCM. Each element is associated with a single ISCM process step, as defined in [SP800-137]. Elements are related to each other by a parent-child relationship if the elements represent the same ISCM concept but in adjacent process steps, as described in SP 800-137A.

For example, the element, “The ISCM strategy addresses security control assessments with a degree of rigor appropriate to risk” is associated with the ISCM *Define* process step. A child element, associated with the ISCM *Establish* process step, is “The ISCM program specifies, for each security control, a frequency for its assessment that is appropriate to risk.” These two elements represent the same ISCM concept at adjacent stages of the ISCM process. The concept is first addressed in the ISCM strategy then addressed in more detail by the ISCM *Establish* process step.

The information fields for the assessment elements are shown in Table 3.

Table 3 – Assessment Element Information Fields

Attribute	Description
Identifier (ID)	The element's unique identifier.
Assessment Element Text	AA statement that should be true for a well-implemented ISCM program.
Level	The risk management level(s) appropriate to evaluate the element (see Section 2.4).
Source	The primary source document for an element's subject matter.
Critical	A Yes/No indicator signifying that an element is of greater importance than non-critical elements. See [SP800-137A] for the criteria for this designation.
Assessment Procedure	A procedure defining the steps to be taken to meet an assessment objective for each assessment element, including one or more determination statements on which to make judgments. Assessment procedures are defined in [SP800-137A].
Discussion	Assistance and explanation to facilitate consistent evaluation of the element. The discussion is taken directly from [Catalog].
Rationale for Level	Rationale for why the assessment element is assigned to a particular risk management level(s).
Parent	The element, if any, associated with the previous process step that represents the same ISCM concept as the current element.

2.4 Incremental Assessments

ISCMA may be used in an incremental fashion, as described in [SP800-137A], to encourage ongoing reassessment of ISCM programs as the programs develop and mature. In this way, ISCM programs can be assessed—regardless of program development state or maturity—with a focus on aspects of the ISCM program that are in place.

ISCMA fully supports incremental assessments that limit the ISCM process steps to be assessed:

- *Define only* for an assessment of the ISCM strategy
- *Define and Establish only* for an assessment of the ISCM program design
- *Define, Establish, and Implement only* for an assessment of the ISCM program implementation
- *All process steps* for full assessment of the entire breadth of the ISCM program

In addition, ISCMA supports incremental assessments of only those elements identified as critical using the criteria defined in [SP800-137A]. The critical assessment elements are not shown in this report but can be found in [ISCMAx] and in the SP 800-137A element catalog [Catalog].

2.5 Risk Management Levels

Risk management levels are defined in [SP800-39] and are fundamental to the evaluation of assessment elements.

- Level 1 personnel are responsible for the organization-wide risk ISCM strategy, policies, procedures, and implementation.
- Level 2 personnel are responsible for the ISCM strategy, policies, procedures, and implementation for specific mission/business functions.
- Level 3 personnel are responsible for ISCM strategy, policies, procedures, and implementation for individual information systems.

In ISCMA, a given assessment element is evaluated separately at one, two, or (in some cases) all three risk management levels. Evaluation at separate levels facilitates the exposure of any miscommunication among the levels. Each level conducts its own ISCMA consisting of all and only the assessment elements specifically assigned to be evaluated at that level. The overall organizational ISCMA is then derived by combining the results from the three levels.

The full scope of an ISCMA engagement determines the scope of the levels. For example, if a Level 2 organization within a larger organization uses ISCMA for itself (i.e., outside of the context of the full organization), then it considers itself Level 1 for the purposes of the ISCMA.

There are two distinct logistical approaches to conducting an ISCMA at Level 2 (or similarly, at Level 3):

a) Each Level 2 organization addresses the Level 2 assessment elements from its own perspective with no consideration for what other Level 2 organizations are doing. This is the preferred approach because the results are more focused, and misunderstandings are more fully exposed. It is particularly well-suited for a distributed self-assessment.

or

b) Multiple Level 2 organizations come together and address the Level 2 assessment elements from a group perspective, using consensus to determine a single judgment for each element. This approach is less accurate but does provide an opportunity for the groups to learn from one another and is frequently used with facilitated engagements.

2.6 Judgments

Following [SP800-137A], the ISCMA uses the term *judgment* for the descriptive evaluation of an element. Each judgment is also mapped to a numeric score that can be used to calculate an overall assessment score.

[SP800-137A] recommends a two-value judgment set consisting of the values Satisfied and Other Than Satisfied while recognizing that additional, more granular judgments may help organizations with prioritizing corrective actions for ISCM program improvements.

An alternate judgment set consisting of four values was developed for ISCMA to facilitate program improvement prioritization. The alternate judgment set consists of the values Mostly / Completely True, Somewhat True, Mostly False, and Completely False.

The alternate judgments for each element provide organizations with a degree of granularity in assessing ISCM accomplishments that fall short of the pure definition of "True." In addition, there is no neutral judgment—a judgment either leans toward true or false.

There is intentionally no distinction between Mostly True and Completely True in order to focus the organization's attention on making progress on its most neglected elements by diverting attention from elements that are being done well but not perfectly. The Completely False judgment is reserved for elements that have not been addressed at all by the organization. If the element is true anywhere in the organization and to any degree, then it is at least Mostly False.

Assessing an element using the provided alternate judgment set or any other granular set begins by determining if the strongest possible judgment (i.e., Mostly / Completely True) is applicable. If the strongest judgment does not apply, then the most appropriate remaining judgment is selected. Use of a more granular judgment set does not add any new information to the resulting assessment since assessors add notes to explain judgment choices regardless of the judgment set used. However, the additional granularity facilitates analysis in ISCMAx, as described in Section 4.6.

The examples throughout this report will illustrate both the recommended and the alternate judgment sets. In addition, ISCMAx is provided in two configurations: one preconfigured for the recommended judgment set and one preconfigured for the alternate judgment set.

2.7 Reporting Views

A *reporting view* (or simply *view*) is a way of arranging assessment elements into groups such that each element is in exactly one group.

Views can be useful as structures for organizing the assessment elements for reporting and analysis. For example, every element is associated with a unique *Process Step*, so separate ISCMA scores can be calculated for each *Process Step* (e.g., a score for *Define*, a score for *Establish*, etc.).

The remainder of this section describes the reporting views defined by ISCMA. [ISCMAx] produces a separate scorecard and graphical report for each view (see Figure 27).

2.7.1 Section View

Section is the default primary reporting view and was created specifically to facilitate navigation through the assessment elements during the ISCMA. The section names are modeled directly after the subject matter of the associated elements. The section names are identical to the labels on the chains in the [Catalog].

When assessment elements are presented for consideration to the ISCMA participants, they must be presented in *some* order, but ISCMA does not prescribe any specific way to organize the elements for conducting the assessment and making judgments. The elements are each self-sufficient and can be addressed in any order. However, considering elements by *Section* is recommended for conducting the ISCMA. For example, all elements related to *ISCM Strategy Management* are considered together, while all elements related to *ISCM Resources* are considered as a separate group.

The full list of sections is shown in Table 4.

Table 4 – Section View

Section Name	Description
ISCM Strategy Management	Elements related to the breadth and depth of the ISCM strategy
System Level Strategy	Elements related specifically to ISCM strategy at the system level
ISCM Program Management	Elements related to the design and management of the ISCM program
Control Assessment Rigor	Elements related to the relationship between control assessments and risk
Security Status Monitoring	Elements related to the monitoring of ISCM data and metrics
Common Control Assessment	Elements related to the assessment of common controls
System-Specific Control Assessment	Elements related to the assessment of system-specific controls
ISCM Results Included in Risk Assessment	Elements related to the use of ISCM in risk assessment

Section Name	Description
Threat Information	Elements related to the awareness and monitoring of cyber threat data
External Service Providers	Elements related to external hosting of assets
Security-Focused Configuration Management	Elements related to the processes for managing security configurations
Impact of Changes to Systems and Environments	Elements related to security impact analysis
External Security Service Providers	Elements related to the relationship between external security service providers and ISCM data
Security Monitoring Tools	Elements related to the procedures for using security monitoring tools
Sampling	Elements related to managing object sampling
Risk Response	Elements related to responses to risks
Ongoing Authorization	Elements related to the use of ISCM metrics to inform decisions about allowing systems to continue to operate on the organization's network
Acquisition Decisions	Elements related to the use of ISCM results in making acquisition decisions
ISCM Resources	Elements related to the processes for managing the ISCM human resources
ISCM Training	Elements related to the provision of training in ISCM
Metrics	Elements related to the regular reporting and use of ISCM metrics
Security Status Reporting	Elements related to the reporting of security status
Data	Elements related to the quality of ISCM data
ISCM Program Governance	Elements related to the approval processes used to manage the ISCM program

2.7.2 Perspective View

Perspective is a view intended to highlight specific themes that are central to ISCM but cut across sections. The list of perspectives is shown in Table 5.

Table 5 – Perspective View

Perspective	Description
Sustainment	Elements that are specifically designed to ensure that the ISCM program endures in the organization
Utilization	Elements that are related to the usefulness of the ISCM program in other business processes
Readiness	Elements that are designed to ensure that the ISCM program results are sufficiently robust to reliably inform ongoing authorization decisions
Adoption	All other elements related to a complete adoption of ISCM into the organization.

2.7.3 Process Step View

The *Process Step* view reflects the SP 800-137 ISCM process step that the element most directly supports and can be useful for analyzing and reporting results. Section 2.4 describes the use of process steps in performing incremental assessments. ISCM process steps are defined in [SP800-137].

2.7.4 CSF Category View

ISCMA includes a mapping of assessment elements to the 23 Cybersecurity Framework (CSF) categories defined in [CSF1.1]. The Category Unique Identifiers are used for the view instead of the category names, which are not unique.[3]

2.8 The ISCMA Process

The ISCMA process is the same for all engagement types in Table 2. The steps of the ISCMA process are:

- Plan the approach
- Evaluate the elements
- Score the judgments
- Analyze the results

[3] For example, both the Respond and Recover functions have an Improvement category.

- Formulate actions

The overall process is depicted in Figure 2.

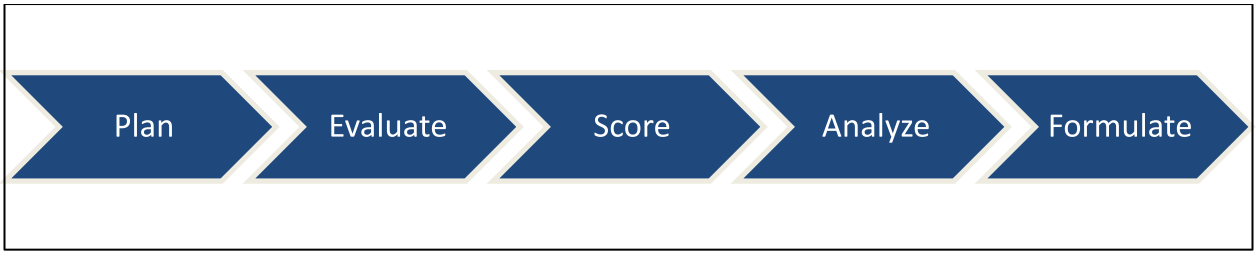


Figure 2 - ISCMA Process

2.8.1 Plan the Approach

Plan
Evaluate
Score
Analyze
Formulate

Figure 3 - ISCMA *Plan the Approach*

There are two depths at which organizations can conduct the ISCMA: *basic* and *detailed*. In a basic assessment, only critical elements are evaluated, while in a detailed assessment, all elements are evaluated. For an organization starting in ISCM or that wants to proceed slowly, the basic assessment is a good place to begin since it is faster and less complex than the full assessment. However, it is recommended that every organization graduate to a detailed assessment as soon as practicable.

Table 6, Table 7, and Table 8 may be useful in planning which depth of assessment to use. The tables assume that the entire breadth of the ISCM program is being assessed.

Table 6 shows the number of elements for each [SP 800-137] ISCM process step, while Table 7 shows the number of elements for each of the seven possible combinations of risk management levels. Table 8 then shows the total number of elements to be considered for each level (e.g., for a full Level 2 assessment, all permutations of levels that include Level 2 are included (2; 1 and 2; 1, 2, and 3) for a total of 49 elements in a detailed assessment and 20 in a basic assessment).

The number of elements is a coarse measure of the level of effort necessary to complete an assessment since any given element may be evaluated after only a quick discussion or may require additional discussion, interviews, or examinations of assessment objects.

Table 6 – Number of Elements by Process Step

Process Step	Detailed Assessment	Basic Assessment
Define	24	9
Establish	43	11
Implement	32	8
Analyze / Report	10	3
Respond	9	1
Review / Update	10	2
Total Elements	**128**	**34**

Table 7 – Number of Elements by Level Combination

Level	Detailed Assessment	Basic Assessment
1	120	33
2	0	0
3	80	18
1 and 2	7	3
1 and 3	0	0
2 and 3	0	0
1 and 2 and 3	72	17
Total Elements	**128**	**34**

Table 8 - Total Judgments by Level

Level	Detailed Assessment	Basic Assessment
1	120	33
2	49	20
3	80	18
Total Judgments	**249**	**71**

An important part of planning is determining how to engage the organization's participants as groups, where a given group performs an assessment for a single risk management level. The minimum number of groups is three, one for each level. For example, if all the appropriate major mission or business unit participants can be brought together, then the group could perform a Level 2 facilitated self-assessment (possibly over several sessions) or participate together in an internal or external engagement with an assessment team.

For internal or external facilitated engagements, there may be a practical limit to how many sessions the assessment team can reasonably undertake, so participant groups are planned accordingly. However, for a distributed self-assessment, there is no such limit. For example, if there are 20 systems, a Level 3 assessment could be conducted by as many as 20 teams (one team for each system) working in parallel. As an extreme example, if each of the 20 teams required three participants, then a Level 3 assessment could be conducted by each person (i.e., 60 assessments in parallel). In any case, where there are multiple assessments for Level 3, they are combined using the rules described in Section 2.8.3.

The ability to scale the assessment to the extent described in the previous paragraph is a key benefit of a distributed self-assessment in a large organization.

An additional planning action is to choose how to resolve conflicts among several judgments at the same risk management level. ISCMA supports the *majority judgment* and the *weakest judgment* methods.

Majority Judgment: The Majority Judgment method is the recommended method and is consistent with the approach taken in [IGMetrics]. The judgment that occurs the greatest number of times is taken as the result. If more than one judgment occurs the greatest number of times, then the weakest judgment is taken as the result.

For example (recommended judgments), suppose that four groups of participants judged a Level 3 element to be *Satisfied* while two groups judged the same element to be *Other Than Satisfied*. In this case, the combined judgment is *Satisfied.*

For example (alternate judgments), suppose that four groups of participants judged a Level 3 element to be *Somewhat True* while two groups judged the same element to be *Mostly False*. In this case, the combined judgment is *Somewhat True*.

Weakest Judgment: The Weakest Judgment method follows the established security principle that a chain is only as strong as its weakest link. The weakest judgment is taken as the result.

For example (recommended judgments), suppose five groups of participants judged a Level 3 element to be *Satisfied* while another group judged the same element to be *Other Than Satisfied*. In this case, the combined judgment is *Other Than Satisfied*.

For example (alternate judgments), suppose five groups of participants judged a Level 3 element to be *Somewhat True* while another group judged the same element to be *Mostly False*. In this case, the combined judgment is *Mostly False*.

Finally, the key decision that is made after evaluating the considerations above is the selection of one of the assessment engagement types described in Section 2.2.

2.8.2 Evaluate the Elements

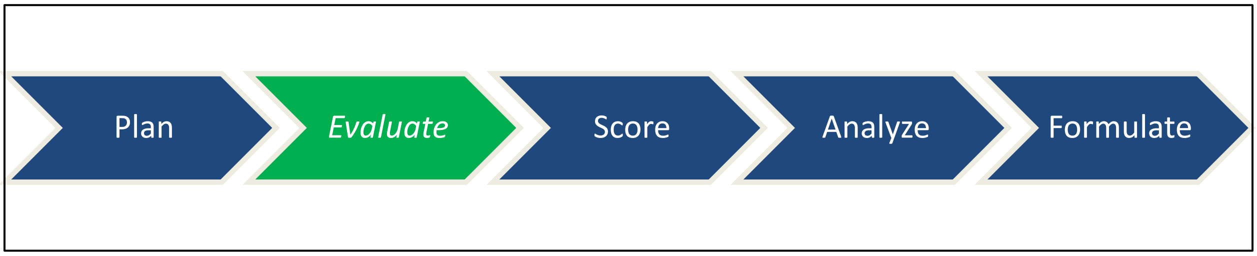


Figure 4 - ISCMA *Evaluate the Elements*

In *Evaluate*, all the required elements are evaluated (judged) by the groups of participants for all the relevant organizational levels. At the end of the *Evaluate* step, multiple assessments at multiple levels are brought together into a single comprehensive assessment in the *Score* step.

Elements can be judged in any order and for any relevant risk management level, providing a great deal of flexibility in organizing the activity across time, location, and resources.

Guidelines for making individual judgments:

- Each valid combination of element and level has a corresponding judgment that is determined without regard to any other elements.

- Each judgment is based on applying one or both of the ISCM program assessment methods identified in [SP800-137A]: *examine*, and *interview*.
- Each element in the elements [Catalog] includes an Assessment Procedure consisting of one or more assessment objectives and a set of potential assessment methods and objects, and a Discussion to provide guidance and clarification for the ISCMA participants. It is important to consider the guidance carefully before making a judgment.
- Making judgments by consensus is done according to the guidance in Section 2.9.

In accordance with [SP800-137A], there is no "Not Applicable" judgment in ISCMA, nor is there provision for selectively excluding elements that do not appear to apply to an organization.

For example, consider element 1-013:[4]

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

If there are no systems/system components hosted by external service providers, the ISMCA participants still judge the element and determine if the topic is addressed by the ISCM strategy if only to document, for example, that there are currently no such systems/system components, that hosting by external providers is not permitted or that if such systems/system components were to become necessary, they would be addressed at that time.

Risk management level may, in some cases, affect the applicability of assessment elements. If an element is applicable to only part of the organization, further organization-specific guidance is necessary to prevent inconsistent approaches to the assessment process for that element.

Ideally, Level 1 is responsible for the ISCM guidance on external providers, but Level 1 may have delegated responsibility for such guidance to Level 2. In this case, consider how the overall Level 2 judgment might be made if all the Level 2 organizations except for X had externally hosted assets. There are three scenarios to consider:

a) If the Level 2 judgment is made by an assessment team conducting a series of interviews, the assessment team would interview X and determine that X had no such guidance for a valid reason and so would not consider X in making the overall Level 2 judgment.
b) If the Level 2 judgment is made by consensus at a meeting of the representatives of all Level 2 missions/business functions, the fact that X had no such assets or published guidance would be discussed and, similarly, would not affect the overall Level 2 judgment.
c) If the Level 2 judgment is made by distributing self-assessments to each Level 2 missions/business functions, X has the dilemma of how to make its own judgment for 2-019 in the absence of a "Not Applicable" choice. Section 2.8.1 describes how multiple judgments at the same level are resolved into an overall judgment. The only judgment that X can make in scenario c that always leads to the same result as in scenarios a and b is to not make any judgment at all. For this reason, ISCMA allows incomplete sets of

[4] The full list of assessment elements can be found in the accompanying tool, [ISCMAx].

judgments in an assessment instance. X simply ignores element 2-019. Note that if the assessment is using the Weakest Judgment method for resolving judgment conflicts at the same risk management level, X could safely make the best possible judgment for element 2-019 since doing so would not affect the overall Level 2 judgment.

2.8.3 Score the Judgments

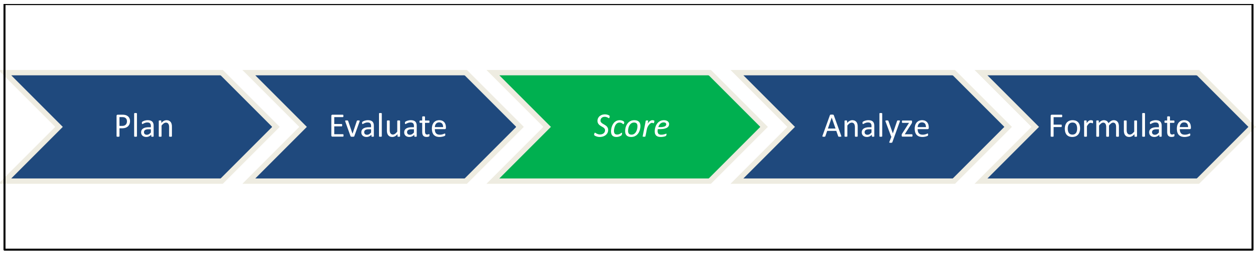


Figure 5 - ISCMA *Score the Judgments*

In the *Score* step, multiple assessments, at multiple levels, are consolidated into a single comprehensive assessment and scored. There are two types of consolidation—*intra-level* and *inter-level*—which are performed in order, element by element.

Intra-level consolidation refers to the combination of multiple judgments for a single element/level. ISCMA resolves intra-level consolidation using the algorithm determined during *Plan the Approach* (see Section 2.8.1).

Inter-level consolidation refers to the combination of judgments for a single element across levels and is done only after intra-level consolidation has been performed for all three risk management levels. ISCMA resolves inter-level conflicts by using specific rules to combine the judgments for Levels 2 and Level 3 and then to combine that result with the judgment for Level 1. The consolidation results in a single judgment for the element.

For example (recommended judgments), if the judgments for Levels 1, 2, and 3 are *Satisfied*, *Other Than Satisfied*, and *Satisfied*, respectively, then Figure 6 shows that the combined Level 2+3 judgment is *Other Than Satisfied*. Then, using the Level 2+3 result as the lower level and Level 1 as the higher level, Figure 6 shows that the final judgment for the element is *Other Than Satisfied.*

	Lower Level	
Higher Level	Satisfied	Other Than Satisfied
Satisfied	**Satisfied**	Other Than Satisfied
Other Than Satisfied	Other Than Satisfied	**Other Than Satisfied**

Figure 6 - Inter-Level Consolidation (Recommended Judgments)

For example (alternate judgments), if the judgments for Levels 1, 2, and 3 are *Somewhat True*, *Mostly False*, and *Completely False*, respectively, then Figure 7 shows that the combined Level

2+3 judgment is *Completely False*. Then, using the Level 2+3 result as the lower level and Level 1 as the higher level, Figure 7 shows that the final judgment for the element is *Mostly False*.

	Lower Level			
Higher Level	Mostly/Completely True	Somewhat True	Mostly False	Completely False
Mostly/Completely True	**Mostly/Completely True**	Somewhat True	Somewhat True	Mostly False
Somewhat True	Somewhat True	**Somewhat True**	Mostly False	Mostly False
Mostly False	Mostly False	Mostly False	**Mostly False**	Completely False
Completely False	Completely False	Completely False	Completely False	**Completely False**

Figure 7 - Inter-Level Consolidation (Alternate Judgments)

In general, the consolidation rules are specified as a table for implementation. However, the rule for the recommended judgment set is easily stated as: if both level judgments are *Satisfied*, the result is Satisfied; otherwise, the result is *Other Than Satisfied*.

The consolidation process is completely automated by the [ISCMAx]tool.

To complete the scoring process, the contributions of judgment scores for the critical elements are weighted more than those of non-critical elements by multiplying the critical element scores by a weighting factor, although weighting of critical elements is relevant only for a detailed assessment where both critical and non-critical elements are assessed. The overall score is then calculated as the total score divided by the maximum possible score and expressed as a percentage:

$$\mathit{Overall\ Score} = 100 * \frac{\sum \mathit{Element\ Scores}}{\sum \mathit{Maximum\ Element\ Scores}}$$

The scoring technique can also be applied to any subset of elements to get additional view-based scores. For example, to get a score for the *Governance* section only, the scores for just the elements in the *Governance* section can be compared with the maximum possible scores for the *Governance* section elements. Additional view-based scores are automatically provided by [ISCMAx] for each reporting view.

2.8.4 Analyze the Results

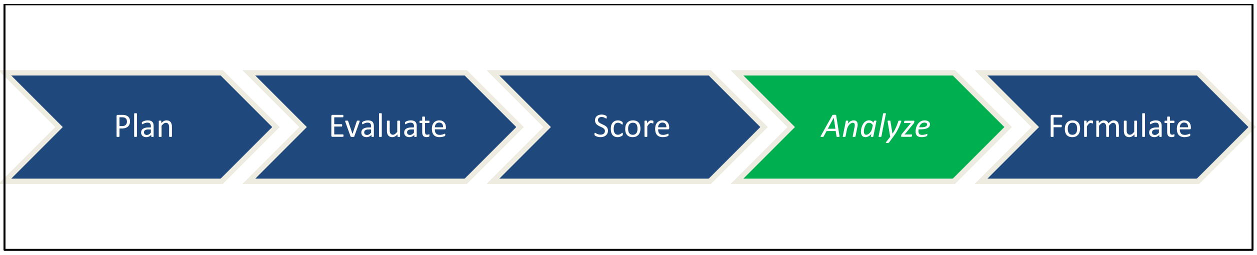


Figure 8 - ISCMA *Analyze the Results*

Once there is a combined judgment and score for each element, the results are analyzed. The following can be reviewed in any order if they exist:

- Elements or sections where the results are weak
- Elements or sections where the results, while not necessarily weak, are weaker than expected
- Elements where the result is weak because of a relatively small number of weak Level 2 or Level 3 contributions
- Elements or sections where there are wide discrepancies among the levels
- Elements that contribute to a weak process step score
- Element or section score improvement over the previous assessment
- Feedback from organization participants
- Feedback from assessment personnel for an external or internal engagement

2.8.5 Formulate Actions

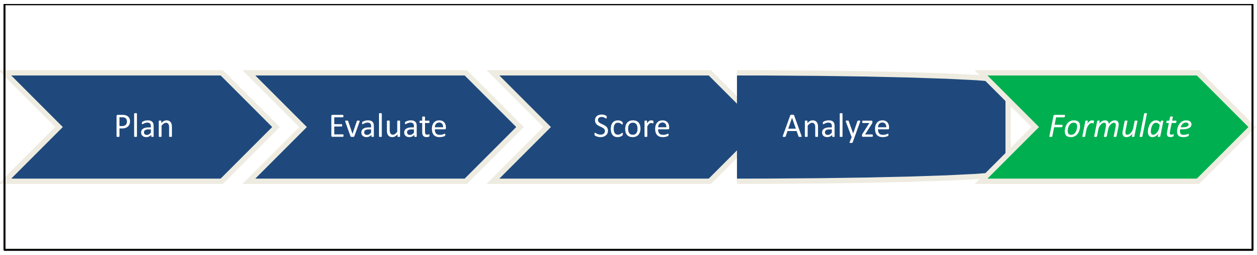


Figure 9 - ISCMA *Formulate Actions*

The final step in the assessment process is to produce actionable recommendations. Actions can be based on the considerations in Section 2.8.4 as well as on:

- Ways to improve the score for the foundational Strategy and Policy section
- One or more additional sections to target for improvement
- Recommendations from the assessment team (for external or internal engagements)
- A timeframe for a follow-up assessment
- A realistic evaluation of how much can be accomplished in a given timeframe
- Assignment of responsibilities for executing each recommendation

2.9 The Use of Consensus

It is extremely important that consensus be used correctly in the context of the ISCMA methodology.

A consensus judgment is one where each of the participants accepts the result even if there is not complete agreement. Consensus is common in group decision-making, but in making a judgment about an ISCM assessment element, it is appropriate only if all of the following are true:

- The scope of the judgment is a single risk management level;
- If the judgment is for Level 2, all participants represent the same mission or business unit; and
- If the judgment is for Level 3, all participants represent the same system.

The conditions will likely not all be true in the context of a distributed self-assessment. The resolution process selected in Section 2.8.1 provides the best achievable result.

For example (recommended judgments), suppose two Level 3 participants representing the same system cannot come to a consensus on an element's judgment because one participant insists on *Satisfied* and the other insists on *Other Than Satisfied*. If the participants are unable to come to a consensus, then the assessment result is as if they had performed the assessment independently (e.g., if the *Weakest Judgment* algorithm is being used, the judgment is *Other Than Satisfied*).

For example (alternate judgments), suppose two Level 3 participants representing the same system cannot come to a consensus on an element's judgment because one participant insists on *Somewhat True* and the other insists on *Mostly False*. If the participants are unable to come to a consensus, then the assessment result is as if they had performed the assessment independently (e.g., if the *Weakest Judgment* algorithm is being used, the judgment is *Mostly False*).

3 ISCMAx: The ISCMA Methodology Assessment Tool

The purpose of [ISCMAx] is to facilitate making, collecting, and consolidating judgments as well as reporting scores and data for analysis and action.

ISCMAx performs the following functions:

- Presents elements by risk management level and allows users to record their judgments;
- Provides element-specific guidance on how to make judgments;
- Allows users to enter additional notes and recommendations for each element;
- Supports the merging of any number of partial assessments into a single master assessment;
- Scores the final master assessment; and
- Provides tables, graphical output, and recommendations to assist the organization in determining its next steps.

3.1 ISCMAx and Excel

[ISCMAx] is a Microsoft Excel-based application that implements ISCMA as described in this report. The ISCMAx tool has been written and tested on the Microsoft Windows OS platform; it is not compatible with Apple OS.

ISCMAx requires Excel 2010 or later. The tool relies heavily on Excel macro code and will not operate with any other spreadsheet than Excel. ISCMAx has been tested with both 32-bit and 64-bit versions of Excel on both 32-bit and 64-bit versions of Windows 10.

No knowledge of Excel is necessary to enter judgments. However, it is assumed in this report that the reader is familiar with the basic concepts of Excel, which are necessary for all other ISCMAx functions. All ISCMAx output is provided in the form of Excel worksheets, and it may be useful to be able to sort and filter within the worksheets. In addition, any tailoring of ISCMAx requires directly modifying data in various worksheets.

3.2 Obtaining ISCMAx

[ISCMAx] consists of a single Excel file. For convenience, ISCMAx is provided as part of a compressed (ZIP) file called "ISCMAx <version>.zip" that contains the following additional example files:

- FullAssessmentSample.xls, the master assessment report resulting from combining the three example assessments
- ISCMAx <version> L3-All.xlsm, a completed Level 3 assessment
- ISCMAx <version> L2-DE.xlsm, a completed Level 2 assessment
- ISCMAx <version> L2-ABC.xlsm, a completed Level 2 assessment
- ISCMAx <version> L1-SAISO.xlsm, a completed Level 1 assessment
- ISCMAx <version> L1-CIO.xlsm, a completed Level 1 assessment

[ISCMAx] can be downloaded at https://csrc.nist.gov/publications/detail/nistir/8212/draft. It may be helpful to have the example files available when reading the rest of this report.

3.3 Overview of ISCMAx Processing

The primary function of [ISCMAx] is to support all engagement types in Table 2 by partially automating the *Evaluate* and *Score* steps of the ISCMA process, as shown in Figure 10:

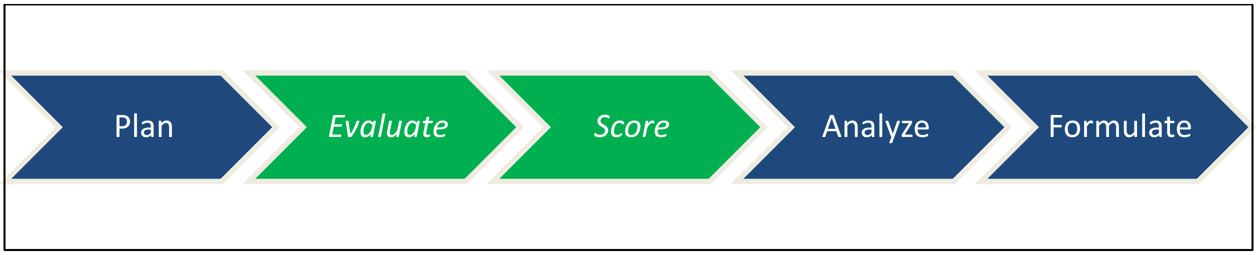


Figure 10 - ISCMA Partially Automated Steps

a) **Evaluate the elements**: ISCMAx allows users to view the elements and their guidance, make judgments, enter notes and recommendations, and record the results.
b) **Score the judgments**: ISCMAx combines the judgments, calculates the scores, and creates a separate Excel workbook called the Master Assessment, which contains the complete assessment results.

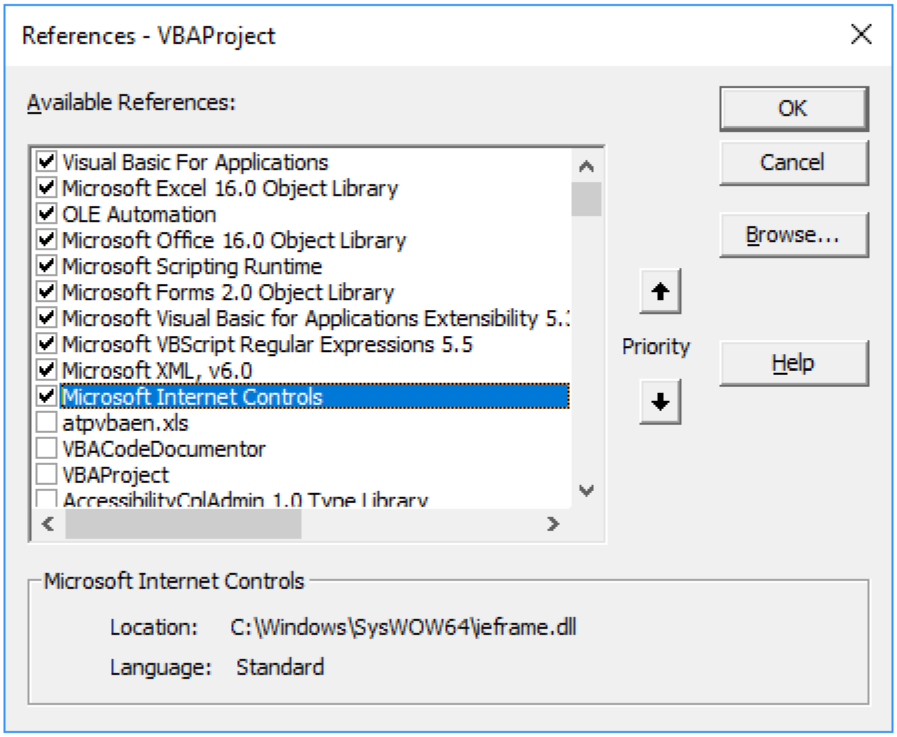
The Master Assessment is discussed in detail in Section 4.

3.4 Starting ISCMAx

The [ISCMAx] application automatically begins running as soon as the workbook is opened.[5]

[5] Depending on local security settings, it may be necessary to click both "Enable Editing" and "Enable Content" at the top of the Excel window before execution can begin.

ISCMAx requires the references shown in Figure 11. If any references are missing, an appropriate error message is displayed. For further assistance, see the Microsoft documentation for References.



References - VBAProject

Available References:

☑ Visual Basic For Applications
☑ Microsoft Excel 16.0 Object Library
☑ OLE Automation
☑ Microsoft Office 16.0 Object Library
☑ Microsoft Scripting Runtime
☑ Microsoft Forms 2.0 Object Library
☑ Microsoft Visual Basic for Applications Extensibility 5.
☑ Microsoft VBScript Regular Expressions 5.5
☑ Microsoft XML, v6.0
☑ Microsoft Internet Controls
☐ atpvbaen.xls
☐ VBACodeDocumentor
☐ VBAProject
☐ AccessibilityCplAdmin 1.0 Type Library

Microsoft Internet Controls

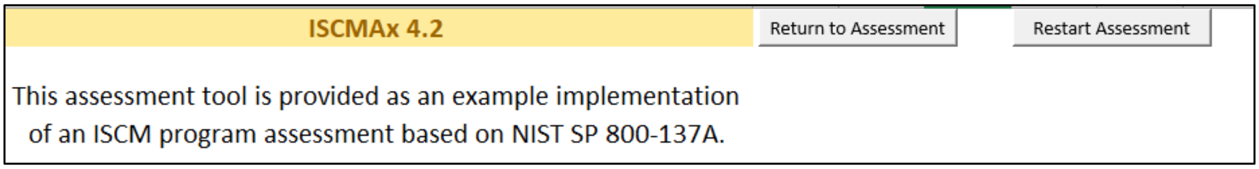
Location: C:\Windows\SysWOW64\ieframe.dll

Language: Standard

Figure 11 - Required References

During the execution of ISCMAx, users interact with Excel forms rather than with worksheets. Most ISCMAx worksheets are hidden, but the *TitlePage*, *Elements,* and *Assessment* worksheets remain visible at all times.

The *TitlePage* worksheet shows the ISCMAx version identifier. If the workbook is already open but ISCMAx has been terminated for some reason, it can be restarted by clicking the *Return to Assessment* button on the worksheet. The assessment can also be restarted from the *TitlePage* worksheet by clicking *Restart Assessment*. This is shown in Figure 12.



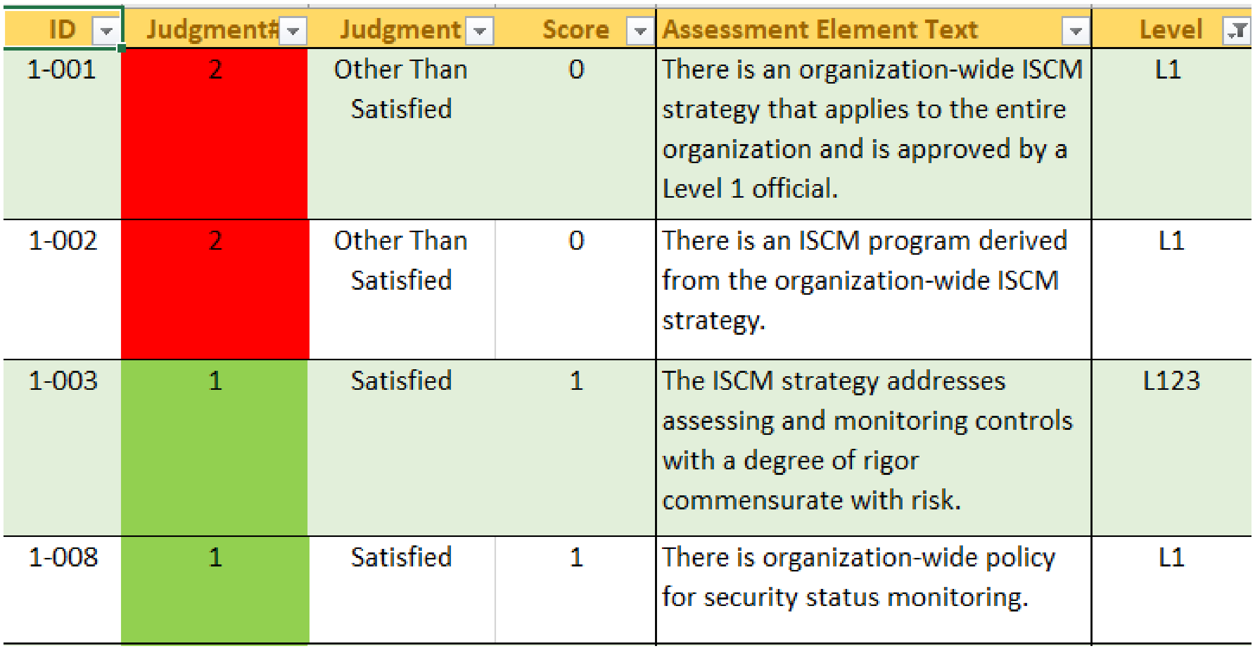
ISCMAx 4.2

This assessment tool is provided as an example implementation of an ISCM program assessment based on NIST SP 800-137A.

Figure 12 - TitlePage Worksheet

The *Assessment* worksheet shows all the data collected for the assessment instance. The *Assessment* worksheet is automatically updated as judgments are made and it is not intended to be edited by users. The *Assessment* worksheet is made visible as an aid to comprehending the assessment process.

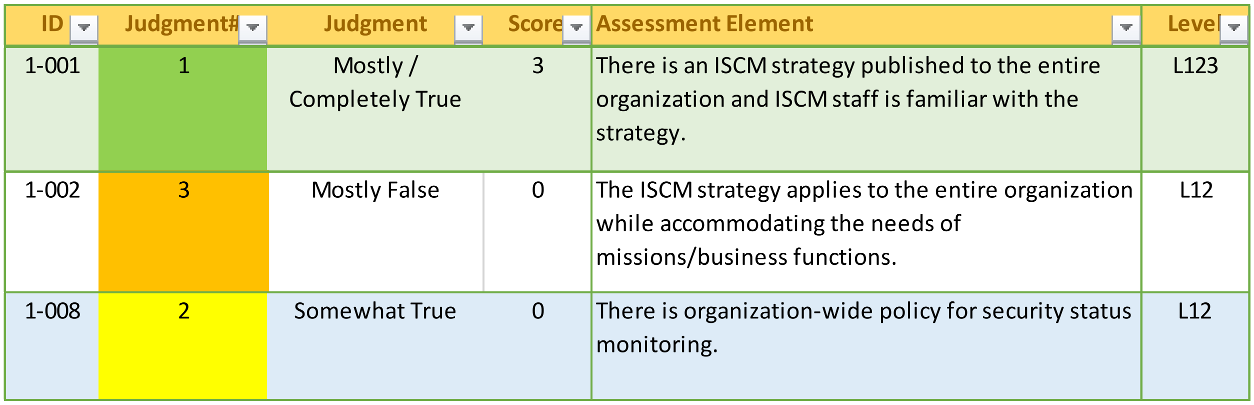
For the recommended judgments, a partial *Assessment* worksheet is shown in Figure 13.



ID	Judgment#	Judgment	Score	Assessment Element Text	Level
1-001	2	Other Than Satisfied	0	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	L1
1-002	2	Other Than Satisfied	0	There is an ISCM program derived from the organization-wide ISCM strategy.	L1
1-003	1	Satisfied	1	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	L123
1-008	1	Satisfied	1	There is organization-wide policy for security status monitoring.	L1

Figure 13 - Assessment Worksheet (Recommended Judgments)

For the alternate judgments, a partial *Assessment* worksheet is shown in Figure 14.



ID	Judgment#	Judgment	Score	Assessment Element	Level
1-001	1	Mostly / Completely True	3	There is an ISCM strategy published to the entire organization and ISCM staff is familiar with the strategy.	L123
1-002	3	Mostly False	0	The ISCM strategy applies to the entire organization while accommodating the needs of missions/business functions.	L12
1-008	2	Somewhat True	0	There is organization-wide policy for security status monitoring.	L12

Figure 14 - Assessment Worksheet (Alternate Judgments)

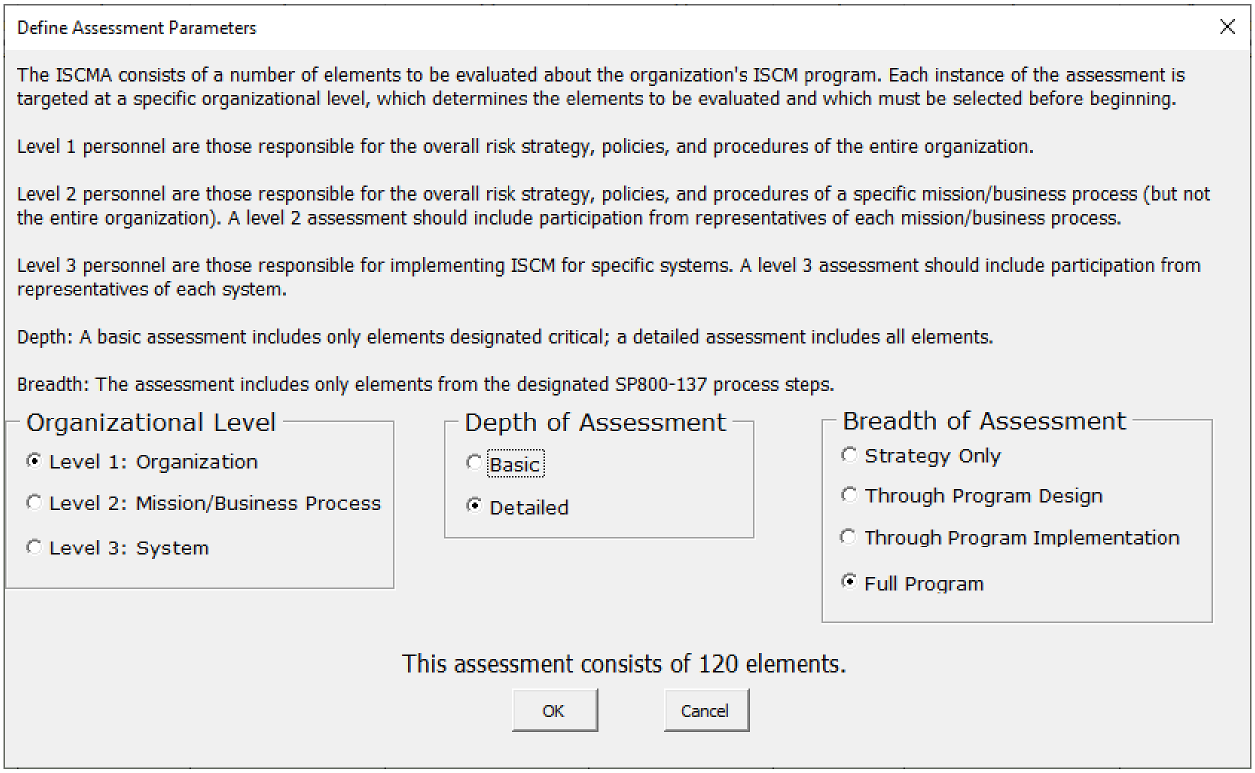
3.5 Assessment Parameters

The elements evaluated during the assessment are determined by the values of three assessment parameters:

1. Risk management level (See Sec. 2.5)
2. Depth (See Sec. 2.8.1)

3. Breadth (See Sec. 2.4)

An example of the assessment parameter selections is shown in Figure 15, which illustrates the Define Assessment Parameters screen that appears when the ISCMAx workbook is opened for the first time. Once the assessment parameters are determined, the assessment proceeds.



Define Assessment Parameters

The ISCMA consists of a number of elements to be evaluated about the organization's ISCM program. Each instance of the assessment is targeted at a specific organizational level, which determines the elements to be evaluated and which must be selected before beginning.

Level 1 personnel are those responsible for the overall risk strategy, policies, and procedures of the entire organization.

Level 2 personnel are those responsible for the overall risk strategy, policies, and procedures of a specific mission/business process (but not the entire organization). A level 2 assessment should include participation from representatives of each mission/business process.

Level 3 personnel are those responsible for implementing ISCM for specific systems. A level 3 assessment should include participation from representatives of each system.

Depth: A basic assessment includes only elements designated critical; a detailed assessment includes all elements.

Breadth: The assessment includes only elements from the designated SP800-137 process steps.

Organizational Level
● Level 1: Organization
○ Level 2: Mission/Business Process
○ Level 3: System

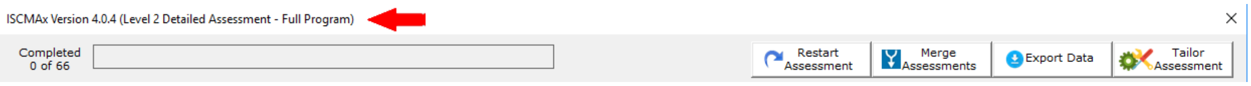
Depth of Assessment
○ Basic
● Detailed

Breadth of Assessment
○ Strategy Only
○ Through Program Design
○ Through Program Implementation
● Full Program

This assessment consists of 120 elements.

Figure 15 - Specifying a Detailed Level 1 Assessment of the Full ISCM Program

The assessment parameters can also be modified later (See Sec. 3.8.1). A formatted display of the current assessment parameters is always shown on the title bar of the assessment screens, as shown in Figure 16.



ISCMAx Version 4.0.4 (Level 2 Detailed Assessment - Full Program)

Completed 0 of 66

Figure 16 - Assessment Parameter Display

3.6 Element Evaluation

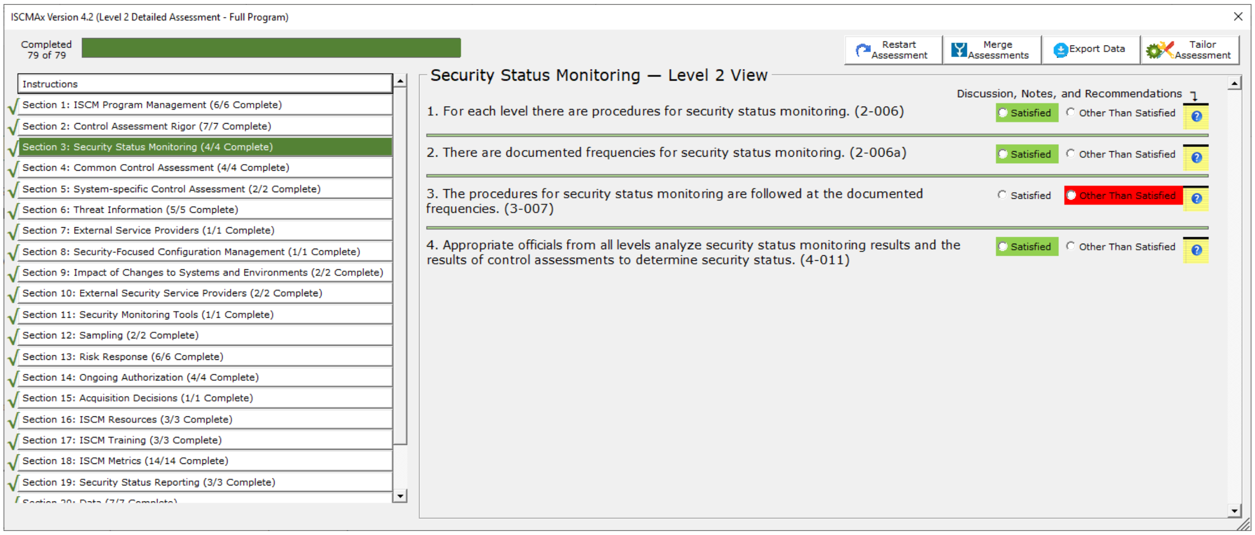
During the assessment, element groups are chosen by section and in any order. Only sections that contain elements corresponding to the current set of assessment parameters are available for selection, as illustrated in Figure 17, which shows a Level 2 detailed assessment with breadth “Through Program Design Only” with only eight of the possible 14 sections visible. None of the hidden sections contain any *Define* or *Establish* elements applicable to Level 2.

Each of the section names that appear on the left side of the screen includes a count of the total number of elements in the section and the number of elements that are already evaluated. The section button is clicked to show and allow evaluation of the elements for the selected section.

Once all elements for a section are evaluated, a check mark appears next to the corresponding section button.

A running count of the number of completed elements and a progress bar are visible above the section buttons.

For recommended judgments, the features described above are shown in Figure 17.


ISCMAx Version 4.2 (Level 2 Detailed Assessment - Full Program)
Restart Assessment
Merge Assessments
Export Data
Tailor Assessment
Instructions
Discussion, Notes, and Recommendations

Completed 79 of 79

- ✓ Section 1: ISCM Program Management (6/6 Complete)
- ✓ Section 2: Control Assessment Rigor (7/7 Complete)
- ✓ Section 3: Security Status Monitoring (4/4 Complete)
- ✓ Section 4: Common Control Assessment (4/4 Complete)
- ✓ Section 5: System-specific Control Assessment (2/2 Complete)
- ✓ Section 6: Threat Information (5/5 Complete)
- ✓ Section 7: External Service Providers (1/1 Complete)
- ✓ Section 8: Security-Focused Configuration Management (1/1 Complete)
- ✓ Section 9: Impact of Changes to Systems and Environments (2/2 Complete)
- ✓ Section 10: External Security Service Providers (2/2 Complete)
- ✓ Section 11: Security Monitoring Tools (1/1 Complete)
- ✓ Section 12: Sampling (2/2 Complete)
- ✓ Section 13: Risk Response (6/6 Complete)
- ✓ Section 14: Ongoing Authorization (4/4 Complete)
- ✓ Section 15: Acquisition Decisions (1/1 Complete)
- ✓ Section 16: ISCM Resources (3/3 Complete)
- ✓ Section 17: ISCM Training (3/3 Complete)
- ✓ Section 18: ISCM Metrics (14/14 Complete)
- ✓ Section 19: Security Status Reporting (3/3 Complete)
- ✓ Section 20: Data (7/7 Complete)

Security Status Monitoring — Level 2 View

1. For each level there are procedures for security status monitoring. (2-006) ● Satisfied ○ Other Than Satisfied

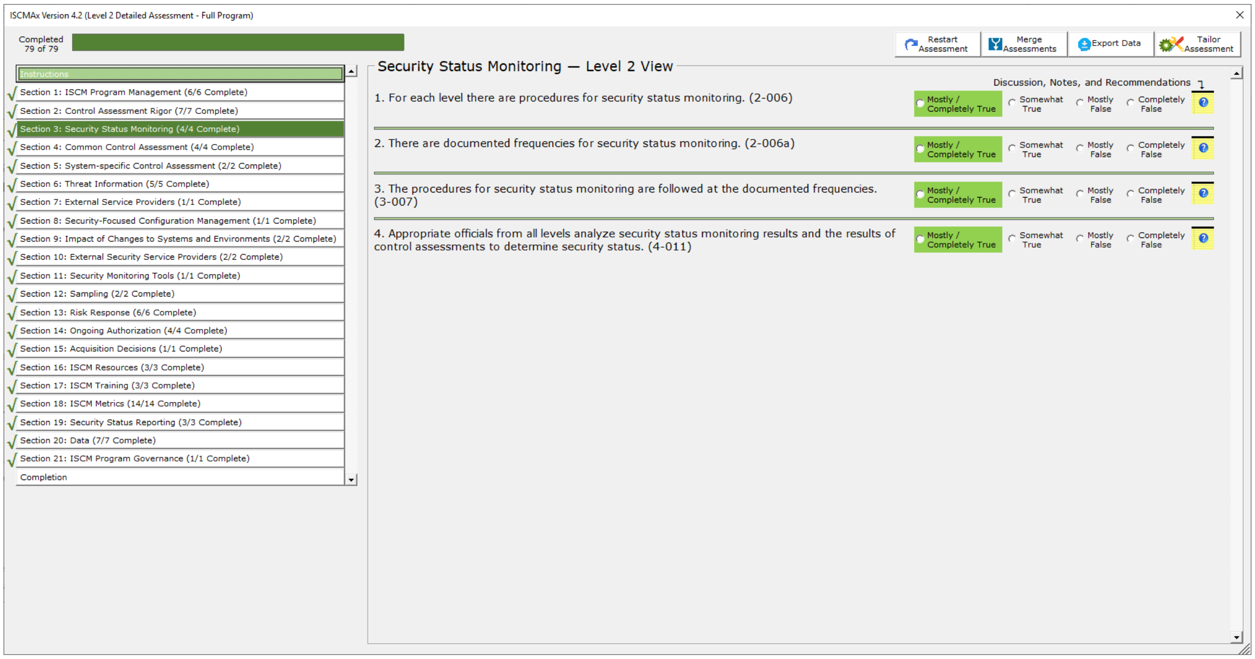
2. There are documented frequencies for security status monitoring. (2-006a) ● Satisfied ○ Other Than Satisfied

3. The procedures for security status monitoring are followed at the documented frequencies. (3-007) ○ Satisfied ● Other Than Satisfied

4. Appropriate officials from all levels analyze security status monitoring results and the results of control assessments to determine security status. (4-011) ● Satisfied ○ Other Than Satisfied

Figure 17 - Element Evaluation Screen (Recommended Judgments)

For alternate judgments, the features described above are shown in Figure 18.



ISCMAx Version 4.2 (Level 2 Detailed Assessment - Full Program)

Completed 79 of 79

- Instructions
- ✓ Section 1: ISCM Program Management (6/6 Complete)
- ✓ Section 2: Control Assessment Rigor (7/7 Complete)
- ✓ Section 3: Security Status Monitoring (4/4 Complete)
- ✓ Section 4: Common Control Assessment (4/4 Complete)
- ✓ Section 5: System-specific Control Assessment (2/2 Complete)
- ✓ Section 6: Threat Information (5/5 Complete)
- ✓ Section 7: External Service Providers (1/1 Complete)
- ✓ Section 8: Security-Focused Configuration Management (1/1 Complete)
- ✓ Section 9: Impact of Changes to Systems and Environments (2/2 Complete)
- ✓ Section 10: External Security Service Providers (2/2 Complete)
- ✓ Section 11: Security Monitoring Tools (1/1 Complete)
- ✓ Section 12: Sampling (2/2 Complete)
- ✓ Section 13: Risk Response (6/6 Complete)
- ✓ Section 14: Ongoing Authorization (4/4 Complete)
- ✓ Section 15: Acquisition Decisions (1/1 Complete)
- ✓ Section 16: ISCM Resources (3/3 Complete)
- ✓ Section 17: ISCM Training (3/3 Complete)
- ✓ Section 18: ISCM Metrics (14/14 Complete)
- ✓ Section 19: Security Status Reporting (3/3 Complete)
- ✓ Section 20: Data (7/7 Complete)
- ✓ Section 21: ISCM Program Governance (1/1 Complete)
- Completion

Security Status Monitoring — Level 2 View

1. For each level there are procedures for security status monitoring. (2-006) ● Mostly / Completely True ○ Somewhat True ○ Mostly False ○ Completely False

2. There are documented frequencies for security status monitoring. (2-006a) ● Mostly / Completely True ○ Somewhat True ○ Mostly False ○ Completely False

3. The procedures for security status monitoring are followed at the documented frequencies. (3-007) ● Mostly / Completely True ○ Somewhat True ○ Mostly False ○ Completely False

4. Appropriate officials from all levels analyze security status monitoring results and the results of control assessments to determine security status. (4-011) ● Mostly / Completely True ○ Somewhat True ○ Mostly False ○ Completely False

Figure 18 - Element Evaluation Screen (Alternate Judgments)

3.6.1 Judgment Selection

To record an element judgment, the appropriate option (radio) button to the right of the element text area is clicked. In addition to recording the value of the judgment, [ISCMAx] changes the color of the judgment for an additional visual confirmation of the selected judgment.[6]

Judgment values are saved immediately—there is no *Save* button on the judgment selection screens. After selecting a judgment, a different selection can be made at any subsequent time and will replace the previous selection.

3.6.2 Element-Level Judgment Assistance

Each element has an associated discussion to assist in making a judgment. The discussion is accessed by clicking on the element's *Notes/Help* icon shown in Figure 19. An example of the resulting *Notes/Help* form is displayed in Figure 20, showing the *Assessment Procedure* for the element, helpful *Discussion* about the element, the *Rationale* for the designated risk management level as well as input areas for *Recommendations* and *Notes* . The *Notes* input area allows the rationale for judgments or other thoughts and considerations to be recorded. The *Recommendations* input area allows recommendations for response to *Other than Satisfied* judgments to be recorded.

[6] The colors of the judgments can be tailored. See Section 5.3.1.

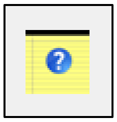
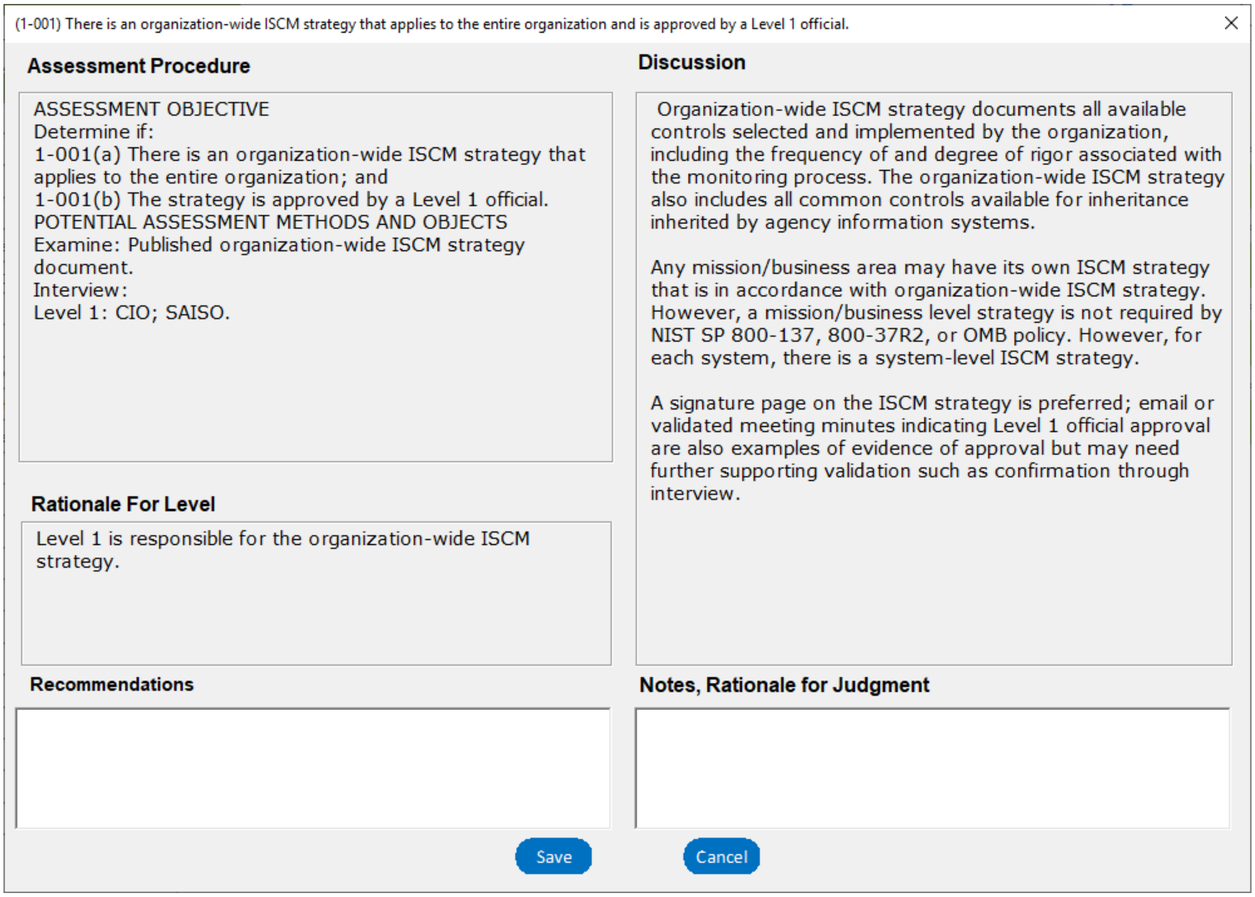


Figure 19 - Notes/Help Icon

Note that there are also buttons for *Save* and *Cancel* on this form.



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

Assessment Procedure

ASSESSMENT OBJECTIVE
Determine if:
1-001(a) There is an organization-wide ISCM strategy that applies to the entire organization; and
1-001(b) The strategy is approved by a Level 1 official.
POTENTIAL ASSESSMENT METHODS AND OBJECTS
Examine: Published organization-wide ISCM strategy document.
Interview:
Level 1: CIO; SAISO.

Discussion

Organization-wide ISCM strategy documents all available controls selected and implemented by the organization, including the frequency of and degree of rigor associated with the monitoring process. The organization-wide ISCM strategy also includes all common controls available for inheritance inherited by agency information systems.

Any mission/business area may have its own ISCM strategy that is in accordance with organization-wide ISCM strategy. However, a mission/business level strategy is not required by NIST SP 800-137, 800-37R2, or OMB policy. However, for each system, there is a system-level ISCM strategy.

A signature page on the ISCM strategy is preferred; email or validated meeting minutes indicating Level 1 official approval are also examples of evidence of approval but may need further supporting validation such as confirmation through interview.

Rationale For Level

Level 1 is responsible for the organization-wide ISCM strategy.

Recommendations

Notes, Rationale for Judgment

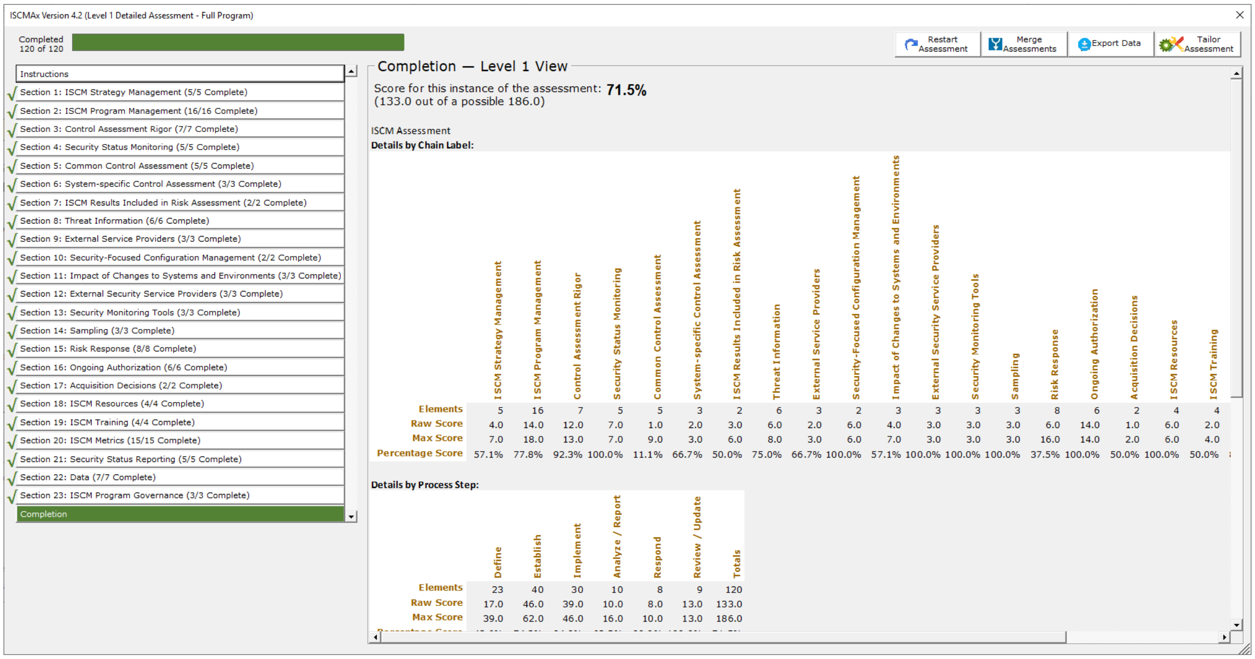
Figure 20 – Element-Level Judgment Assistance

3.7 Scoring and Partial Results

Using recommended judgments, ISCMAx assigns a score of 1.0 for each element judged *Satisfied*. *Other Than Satisfied* judgments are scored 0.0.

Using alternate judgments, ISCMAx assigns a score of 1.0 for each element judged *Mostly / Completely True*. All other judgments are scored 0.0.

Each score is multiplied by its weighting factor (3.0 for critical elements, 1.0 for non-critical elements). The total score is then divided by the maximum possible score to produce a percentage score. The scoring function is illustrated in Figure 21, which shows the result of clicking on the *Completion* button (just below the section buttons).



ISCMAx Version 4.2 (Level 1 Detailed Assessment - Full Program)

Completed 120 of 120

- Instructions
- ✓ Section 1: ISCM Strategy Management (5/5 Complete)
- ✓ Section 2: ISCM Program Management (16/16 Complete)
- ✓ Section 3: Control Assessment Rigor (7/7 Complete)
- ✓ Section 4: Security Status Monitoring (5/5 Complete)
- ✓ Section 5: Common Control Assessment (5/5 Complete)
- ✓ Section 6: System-specific Control Assessment (3/3 Complete)
- ✓ Section 7: ISCM Results Included in Risk Assessment (2/2 Complete)
- ✓ Section 8: Threat Information (6/6 Complete)
- ✓ Section 9: External Service Providers (3/3 Complete)
- ✓ Section 10: Security-Focused Configuration Management (2/2 Complete)
- ✓ Section 11: Impact of Changes to Systems and Environments (3/3 Complete)
- ✓ Section 12: External Security Service Providers (3/3 Complete)
- ✓ Section 13: Security Monitoring Tools (3/3 Complete)
- ✓ Section 14: Sampling (3/3 Complete)
- ✓ Section 15: Risk Response (8/8 Complete)
- ✓ Section 16: Ongoing Authorization (6/6 Complete)
- ✓ Section 17: Acquisition Decisions (2/2 Complete)
- ✓ Section 18: ISCM Resources (4/4 Complete)
- ✓ Section 19: ISCM Training (4/4 Complete)
- ✓ Section 20: ISCM Metrics (15/15 Complete)
- ✓ Section 21: Security Status Reporting (5/5 Complete)
- ✓ Section 22: Data (7/7 Complete)
- ✓ Section 23: ISCM Program Governance (3/3 Complete)
- Completion

Completion — Level 1 View

Score for this instance of the assessment: **71.5%**
(133.0 out of a possible 186.0)

ISCM Assessment
Details by Chain Label:

	ISCM Strategy Management	ISCM Program Management	Control Assessment Rigor	Security Status Monitoring	Common Control Assessment	System-specific Control Assessment	ISCM Results Included in Risk Assessment	Threat Information	External Service Providers	Security-Focused Configuration Management	Impact of Changes to Systems and Environments	External Security Service Providers	Security Monitoring Tools	Sampling	Risk Response	Ongoing Authorization	Acquisition Decisions	ISCM Resources	ISCM Training
Elements	5	16	7	5	5	3	2	6	3	2	3	3	3	3	8	6	2	4	4
Raw Score	4.0	14.0	12.0	7.0	1.0	2.0	3.0	6.0	2.0	6.0	4.0	3.0	3.0	3.0	6.0	14.0	1.0	6.0	2.0
Max Score	7.0	18.0	13.0	7.0	9.0	3.0	6.0	8.0	3.0	6.0	7.0	3.0	3.0	3.0	16.0	14.0	2.0	6.0	4.0
Percentage Score	57.1%	77.8%	92.3%	100.0%	11.1%	66.7%	50.0%	75.0%	66.7%	100.0%	57.1%	100.0%	100.0%	100.0%	37.5%	100.0%	50.0%	100.0%	50.0%

Details by Process Step:

	Define	Establish	Implement	Analyze / Report	Respond	Review / Update	Totals
Elements	23	40	30	10	8	9	120
Raw Score	17.0	46.0	39.0	10.0	8.0	13.0	133.0
Max Score	39.0	62.0	46.0	16.0	10.0	13.0	186.0

Figure 21 - Score Summary

The screenshot in Figure 21 shows two views: *Section (Chain Label)* and *Process Step*. The remaining views are accessed by using the scrollbar. Each view has the same total score, 71.5 %. The difference between the two views is in the scores for the individual items that comprise each view.

Note that the score shown is an example for a Level 1 assessment. In a distributed self-assessment, there may be other Level 1 assessment files, and, in any case, there are additional Level 2 and Level 3 assessment files that are consolidated to produce an overall organizational score. Consolidation and scoring are discussed in Section 4.

3.8 Action Buttons

The top of the ISCMAx assessment form has four *action buttons* shown in Figure 22 and discussed in the subsections below.

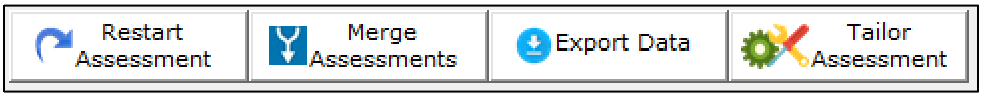


Figure 22 - Action Buttons

3.8.1 Restart Assessment

The *Restart Assessment* action allows modification of the three assessment parameters—risk management level, depth, and breadth—that are described in Section 3.5.

Modifying depth or breadth affects which elements are displayed but does not delete any judgments that may have already been made. Elements are simply hidden or made visible as appropriate to the new parameter values. For example, if a detailed assessment is started, changed to a basic assessment, then changed back again to a detailed assessment, any judgments made—even those made prior to the first change—are still displayed.

Modifying the risk management level in an assessment instance causes the assessment to start over with no judgments. If saving the previous judgments is desired, the workbook should be saved prior to modifying the risk management level.

3.8.2 Merge Assessments

The *Merge Assessments* action initiates the consolidation of multiple assessment files and is discussed in detail in Section 4.

3.8.3 Export Data

The *Export Data* action creates a new Excel workbook containing the data from the current assessment file. The new workbook contains copies of the values (not formulas) in both the *Assessment* (See Figure 14) and *ScoreSummary* (See Figure 21) worksheet. The exported data can then be used by the organization for further analysis or reporting.

3.8.4 Tailor Assessment

The *Tailor Assessment* action unhides the worksheets that are used to tailor the assessment. Tailoring is done prior to conducting the assessment. See Section 5 for a full discussion of tailoring the assessment.

3.9 Deploying the Workbook

The workbook is deployed according to the type of assessment engagement and the logistics for conducting the assessment that were determined during the *Plan the Approach* step of ISCMA. The workbook is deployed within each risk management level and to each group or person expected to make judgments individually. In a group setting, one person is selected to record the group judgments in the workbook.

> It is important that the workbook be deployed only after any desired tailoring is performed. All workbooks used in the assessment are derived from the same tailored template; otherwise, the results are unpredictable.

To create a fresh assessment file for deployment, run the *DeployAssessment* macro[7] from the final tailored version. The resultant file requires the user who opens it to specify all assessment parameters.

[7] The *DeployAssessment* macro is available from the Deployment module, visible from View/Macros.

3.10 Additional Underlying Worksheets

In addition to the *TitlePage*, *Elements*, and *Assessment* worksheet, there are other worksheets used by ISCMAx that are hidden because they are normally not meant to be seen or updated. However, they are temporarily exposed when tailoring is performed. The worksheets are all briefly described in Table 9. For a complete discussion of how the worksheets are used in tailoring, see the appropriate subsections of Section 5.

The worksheet can be tailored except where noted.

Table 9 - Underlying Worksheets

Worksheet	Description
Elements	The source data—all elements and their attributes
Store	Storage for tailoring parameters
Assessment	A filtered copy (based on the current assessment parameters) of the *Elements* worksheet that is used while the assessment is conducted and that also stores judgments and scores; the assessment worksheet is automatically updated **DO NOT MODIFY**
Instructions	The text shown when the *Instructions* button is clicked (and when ISCMAx starts)
JudgmentTable	The table that defines how judgments are combined across risk management levels

4 The Master Assessment Workbook

The *Master Assessment* workbook is a single workbook that combines all the results from all the instances of the assessment created during the assessment process. A separate merge process produces the scores and final assessment report in the worksheets of the *Master Assessment* workbook that are described in this section.

4.1 The Merge Process

The merge process is a separate process invoked by clicking the *Merge Assessments* action button. It creates a new workbook called the *Master Assessment* workbook containing all the judgments, notes, and recommendations from all the workbooks used in the assessment. This data is examined, scored, and organized by the merge process to produce a final assessment report.

Prior to invoking the *Merge Assessments* action, all assessment workbooks are moved or copied into a single folder by the user called the *working* folder. The *Merge Assessments* action is then invoked from any workbook in the working folder, and the assessment workbook from which the *Merge Assessments* action is invoked is then referred to as the *base assessment*. The *Merge Assessments* process examines each workbook in the working folder for compatibility with the version, depth, and breadth of the workbook from which the *Merge Assessments* action is invoked. Unrecognized or incompatible files in the working folder are ignored (with appropriate error messages).

The newly created *Master Assessment* workbook is placed in the working folder and consists of the worksheets listed in Table 10. The worksheets are described more fully in subsequent sub-sections.

Table 10 - Master Assessment Worksheets

Worksheet	Description
ScoreSummary	Tables and graphical displays of scores for all views
Differences	A description of any element found in input assessments that differs from the corresponding element in the base assessment
Messages	Progress, warning, and error messages about the merge process
Observations	All automatically identified conditions detected during the merge process that are reviewed for possible action; see Section 4.5 for the conditions that are reported here
[Single Judgments]	One worksheet for each possible judgment that collects all elements with that judgment as the consolidated judgment
Notes and Recommendations	The collection of all elements in input assessments where there was a note or recommendation
MasterAssessment	The full set of elements for the assessment together with the consolidated judgments made at each level
Level1	All the Level 1 judgments from all the Level 1 input assessments
Level2	All the Level 2 judgments from all the Level 2 input assessments
Level3	All the Level 3 judgments from all the Level 3 input assessments
Chains	Graphical grouping of elements by the is-a-parent-of relationship
JudgmentTable	Codified table that implements the algorithm for combining judgments from different levels

Due to the number of worksheets, it may be necessary to scroll across the list of worksheets using the small arrows shown in Figure 23.

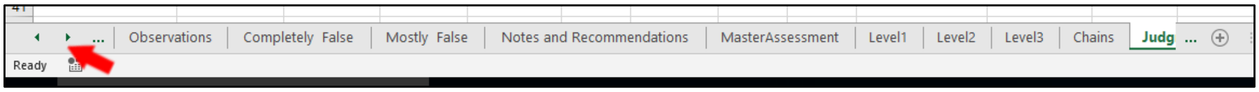


Figure 23 - Master Assessment Worksheet List

Figure 24 shows a diagram of the merge process.

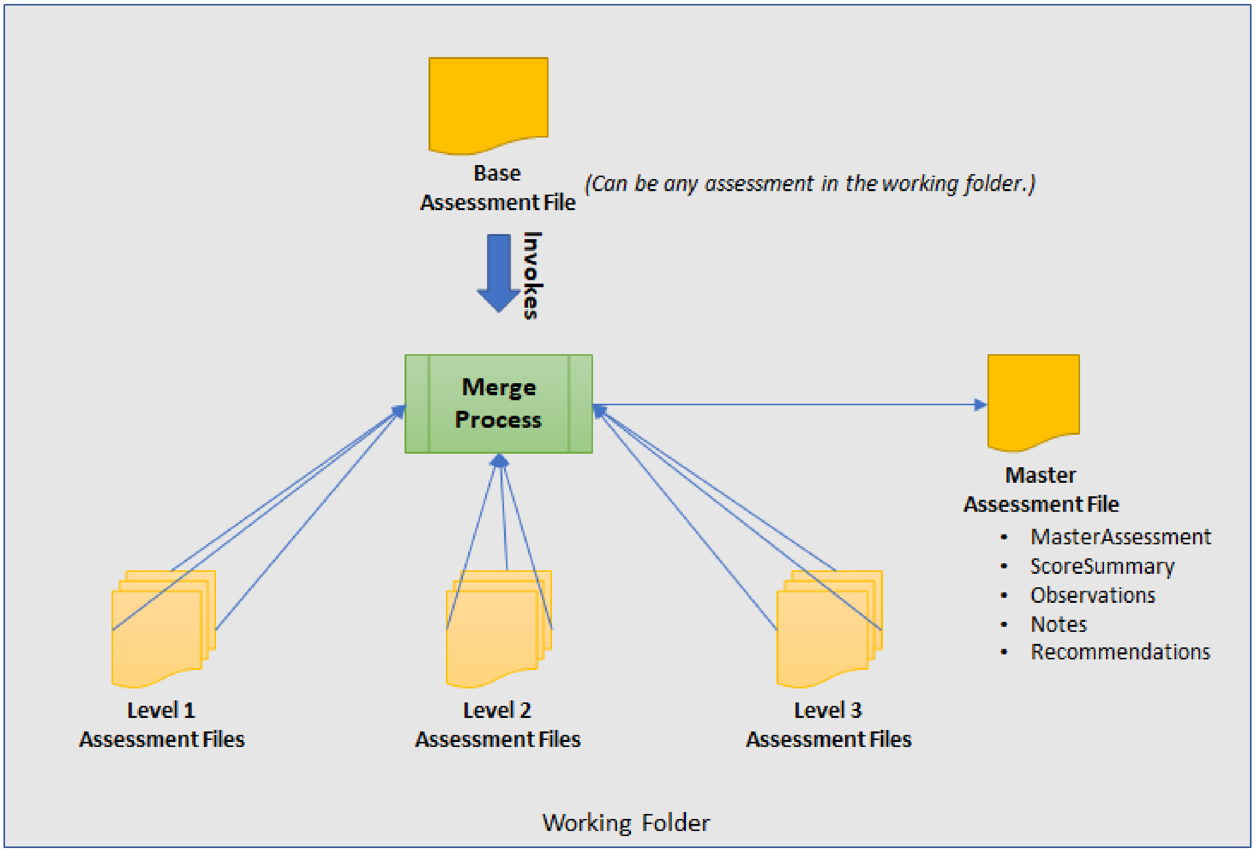
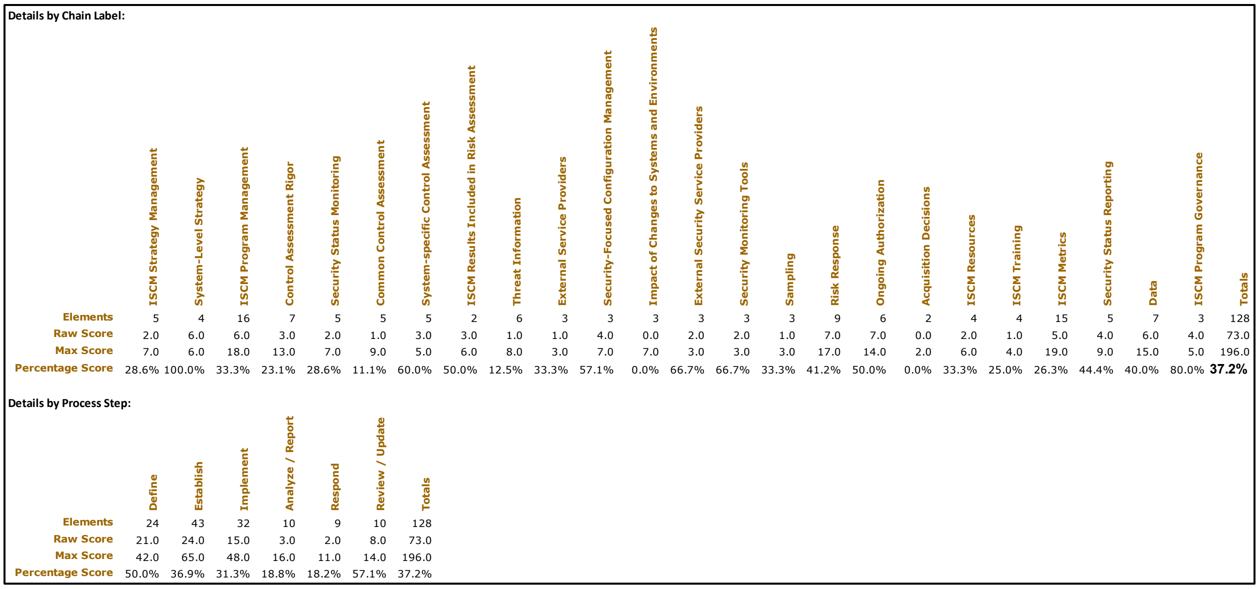


Figure 24 - Merge Process

The merge process can be invoked at any time to see intermediate results as soon as there is at least one judgment for each element at each applicable level. The merge process is then invoked one last time after all necessary assessment workbooks are complete and present in the working folder.

4.2 ScoreSummary Worksheet

The *ScoreSummary* worksheet in the master assessment workbook, shown in Figure 25, provides the same view-based scoring output as shown in Figure 21 for assessment files. The scores in Figure 21 are based on a single workbook that contains a set of judgments for a single level, while the scores in Figure 25 are based on the consolidated judgments for the entire organization.



Details by Chain Label:

	ISCM Strategy Management	System-Level Strategy	ISCM Program Management	Control Assessment Rigor	Security Status Monitoring	Common Control Assessment	System-specific Control Assessment	ISCM Results Included in Risk Assessment	Threat Information	External Service Providers	Security-Focused Configuration Management	Impact of Changes to Systems and Environments	External Security Service Providers	Security Monitoring Tools	Sampling	Risk Response	Ongoing Authorization	Acquisition Decisions	ISCM Resources	ISCM Training	ISCM Metrics	Security Status Reporting	Data	ISCM Program Governance	Totals
Elements	5	4	16	7	5	5	5	2	6	3	3	3	3	3	3	9	6	2	4	4	15	5	7	3	128
Raw Score	2.0	6.0	6.0	3.0	2.0	1.0	3.0	3.0	1.0	1.0	4.0	0.0	2.0	2.0	1.0	7.0	7.0	0.0	2.0	1.0	5.0	4.0	6.0	4.0	73.0
Max Score	7.0	6.0	18.0	13.0	7.0	9.0	5.0	6.0	8.0	3.0	7.0	7.0	3.0	3.0	3.0	17.0	14.0	2.0	6.0	4.0	19.0	9.0	15.0	5.0	196.0
Percentage Score	28.6%	100.0%	33.3%	23.1%	28.6%	11.1%	60.0%	50.0%	12.5%	33.3%	57.1%	0.0%	66.7%	66.7%	33.3%	41.2%	50.0%	0.0%	33.3%	25.0%	26.3%	44.4%	40.0%	80.0%	**37.2%**

Details by Process Step:

	Define	Establish	Implement	Analyze / Report	Respond	Review / Update	Totals
Elements	24	43	32	10	9	10	128
Raw Score	21.0	24.0	15.0	3.0	2.0	8.0	73.0
Max Score	42.0	65.0	48.0	16.0	11.0	14.0	196.0
Percentage Score	50.0%	36.9%	31.3%	18.8%	18.2%	57.1%	37.2%

Figure 25 - ScoreSummary Worksheet

In addition, two types of visualizations—the *Score Summary Bar* and the *View Scorecards*—are provided to assist in the analysis of the results. Each visualization type is composed of the same data presented by the corresponding tabular output in Figure 25.

For the *Score Summary Bar* visualization shown in Figure 26, the vertical location of a target symbol (⦿) represents the overall score of the organization. The top of the bar represents 100 %. To the right, using the same vertical scale are individual view-based visualizations where the vertical location of each view item name indicates the score for that item. The bar is color-coded according to ranges and colors that are configurable.

For the *View Scorecards* visualization, a *View Scorecard* radar chart, shown in Figure 27, is inserted for each reporting view. Data points closer to the outer boundary represent stronger scores. The *View Scorecard* uses the same colors as the *Score Summary Bar*, as well as a configurable set of symbols representing the scoring ranges.

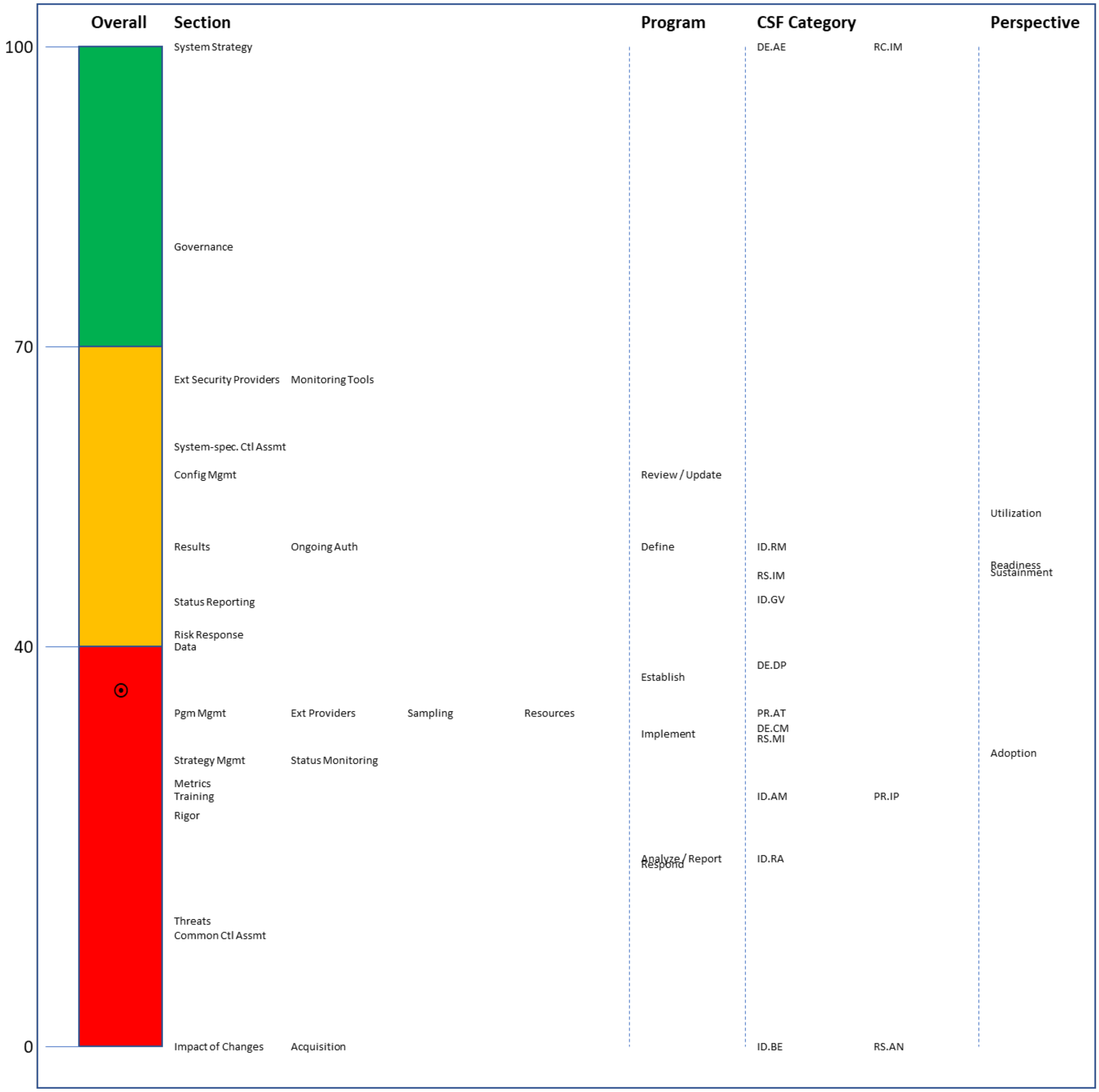
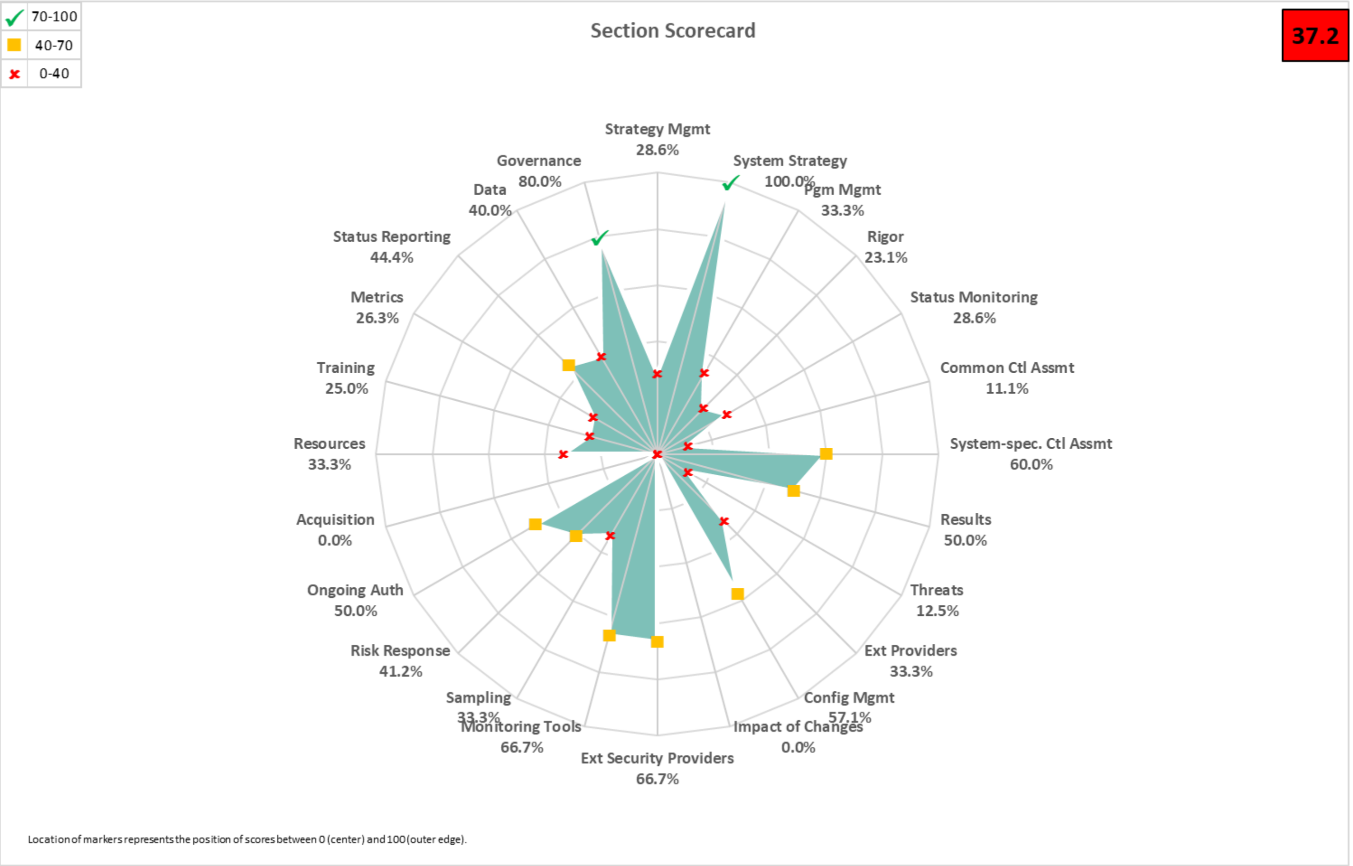


Figure 26 – Score Summary Bar

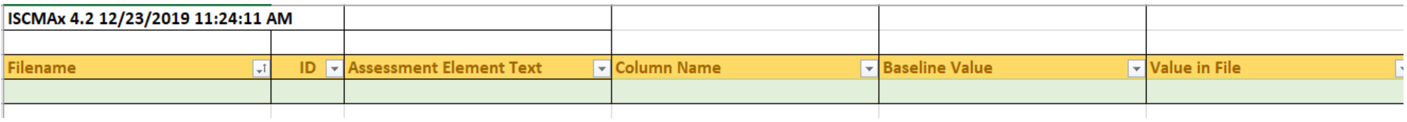


Location of markers represents the position of scores between 0 (center) and 100 (outer edge).

Figure 27 - View Scorecard

4.3 Differences Worksheet

One of the tests conducted during the merge process is a comparison of the base assessment and each of the other workbooks in the working folder. Any field of any element that is critical to matching assessments and that does not match the base assessment is recorded in the *Differences* worksheet. The *Differences* worksheet is reviewed for unexpected information. Organizational managers responsible for the assessment determine if the differences are acceptable. If not, the abnormal assessment files are removed from the working folder, and the merge process is re-executed. An example *Differences* worksheet is shown in Figure 28.

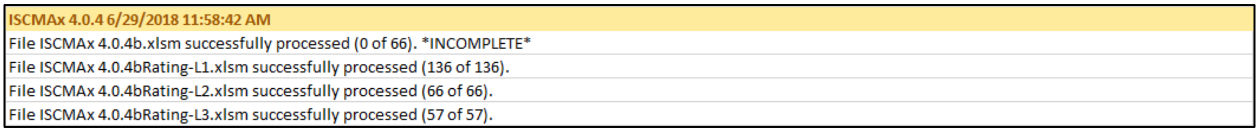


ISCMAx 4.2 12/23/2019 11:24:11 AM					
Filename	ID	Assessment Element Text	Column Name	Baseline Value	Value in File

Figure 28 - Differences Worksheet

4.4 Messages Worksheet

As the merge process proceeds, status messages are produced in the *Messages* worksheet. The *Messages* worksheet, shown in Figure 29, is reviewed for possible unexpected messages before considering the results to be complete and correct. For example, a message might state that a particular assessment workbook does not contain judgments for the entire assessment.



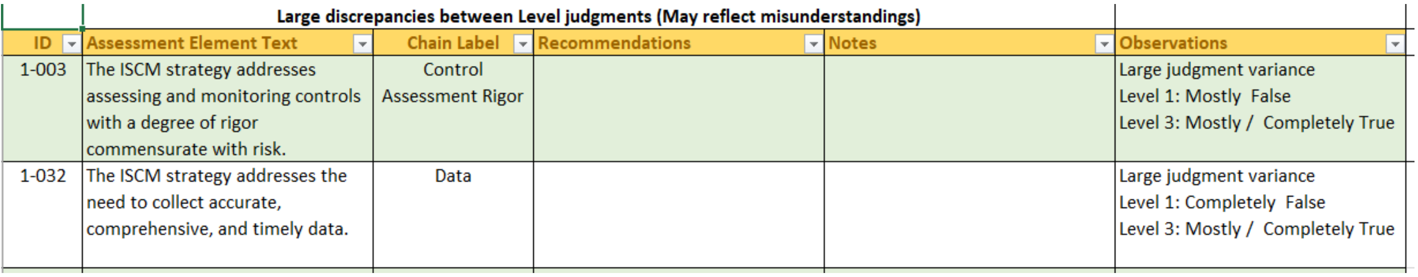
```
ISCMAx 4.0.4 6/29/2018 11:58:42 AM
File ISCMAx 4.0.4b.xlsm successfully processed (0 of 66). *INCOMPLETE*
File ISCMAx 4.0.4bRating-L1.xlsm successfully processed (136 of 136).
File ISCMAx 4.0.4bRating-L2.xlsm successfully processed (66 of 66).
File ISCMAx 4.0.4bRating-L3.xlsm successfully processed (57 of 57).
```

Figure 29 - Messages Worksheet

4.5 Observations Worksheet

The *Observations* worksheet, shown in Figure 30, displays automatically detected conditions that may merit further consideration by the assessment team. The following types of conditions are detected:

- **Widely disparate judgments across risk management levels**: One row is written for each instance of an element where two risk management level judgments are non-adjacent. For example, using alternate judgments, Level 2 indicates *Somewhat True,* but Level 3 indicates *Completely False*. Observations regarding widely disparate judgments are made only if ISCMAx is configured to use a judgment set with three or more judgments.
- **Level judgments determined by a single assessment worksheet**: If a single assessment worksheet among multiple worksheets for one risk management level determines an element's overall judgment, one line is written. Observations regarding judgments determined by a single assessment worksheet are only made if ISCMAx is configured to use *weakest judgment* for intra-level judgment resolution. For example, if Level 2 is represented by six missions/business processes, an observation is written if five missions/business processes assess an element identically while the sixth mission/business process assesses the element more weakly. The *weakest judgment* method causes the judgment made by the sixth mission/business process alone to determine the overall Level 2 judgment for that element.



Large discrepancies between Level judgments (May reflect misunderstandings)

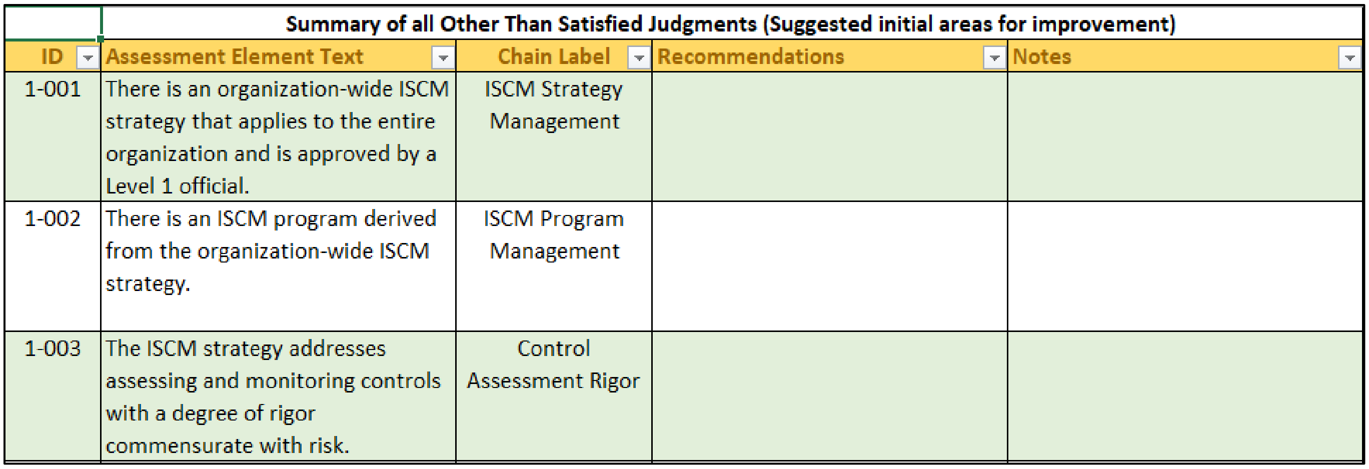
ID	Assessment Element Text	Chain Label	Recommendations	Notes	Observations
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	Control Assessment Rigor			Large judgment variance Level 1: Mostly False Level 3: Mostly / Completely True
1-032	The ISCM strategy addresses the need to collect accurate, comprehensive, and timely data.	Data			Large judgment variance Level 1: Completely False Level 3: Mostly / Completely True

Figure 30 - Observation Worksheet

4.6 Single Judgment Worksheets

The single judgment worksheets are named using the configured judgment labels. Each single-judgment worksheet collects all the elements with the corresponding judgment. This is intended to aid in focusing attention on specific strengths or weaknesses of the ISCM program.

For example, using recommended judgments, all the *Other Than Satisfied* judgments are collected in a single worksheet to facilitate further action. An *Other Than Satisfied* worksheet is illustrated in Figure 31.

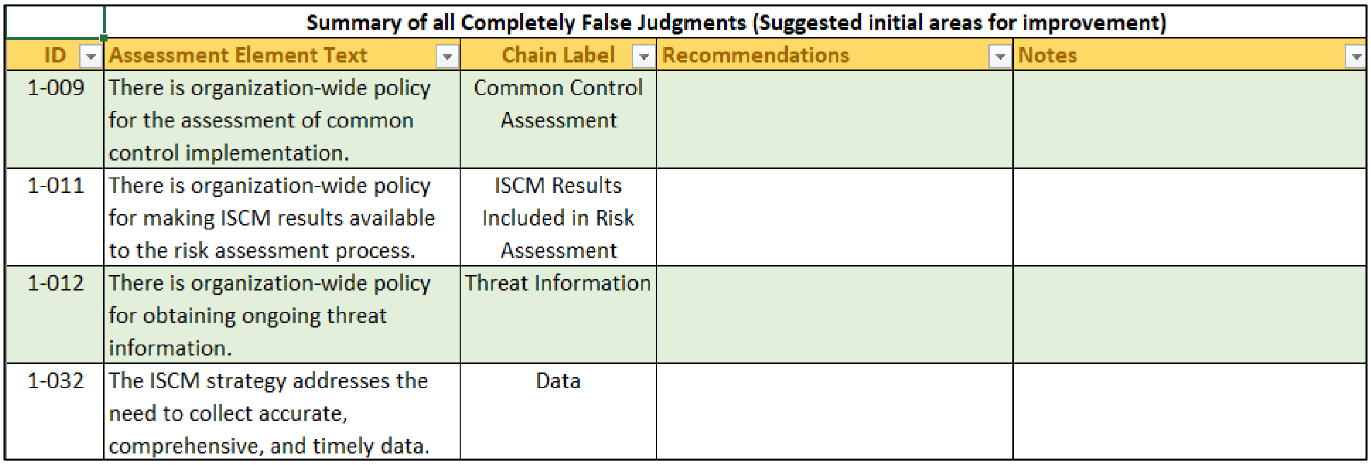


Summary of all Other Than Satisfied Judgments (Suggested initial areas for improvement)

ID	Assessment Element Text	Chain Label	Recommendations	Notes
1-001	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	ISCM Strategy Management		
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	ISCM Program Management		
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	Control Assessment Rigor		

Figure 31 - Other Than Satisfied Worksheet (Recommended Judgments)

For example, using alternate judgments, the *Completely False* judgments are collected in a single worksheet that may be of highest priority because they are the weakest points of the program. Additionally, the *Somewhat True* judgments are collected in a single worksheet that may be the highest priority because they can be improved to achieve a higher score more quickly. The granularity of the alternate judgments is an asset for this analysis. A *CompletelyFalse* worksheet is illustrated in Figure 32.



Summary of all Completely False Judgments (Suggested initial areas for improvement)

ID	Assessment Element Text	Chain Label	Recommendations	Notes
1-009	There is organization-wide policy for the assessment of common control implementation.	Common Control Assessment		
1-011	There is organization-wide policy for making ISCM results available to the risk assessment process.	ISCM Results Included in Risk Assessment		
1-012	There is organization-wide policy for obtaining ongoing threat information.	Threat Information		
1-032	The ISCM strategy addresses the need to collect accurate, comprehensive, and timely data.	Data		

Figure 32 - CompletelyFalse Worksheet (Alternate Judgments)

Any notes or recommendations made by participants during the recording of judgments are included in the single judgment worksheets with each identified by the sequence number of the source assessment file.

4.7 Notes and Recommendations Worksheet

The *Notes and Recommendations* worksheet collects all elements that include notes or recommendations made by participants in any assessment worksheets that contribute to the full assessment. The *Notes and Recommendations* worksheet facilitates finding notes and recommendations without knowing the elements about which they were made, as well as providing a basis for creating action items. Each note/recommendation is preceded by the numeric identifier of the source assessment worksheet of the note/recommendation. The numeric identifiers are defined in the column headings in each of the worksheets *Level1*, *Level2*, or *Level3* (see Section 4.10).

4.8 Relative Judgment Numbers

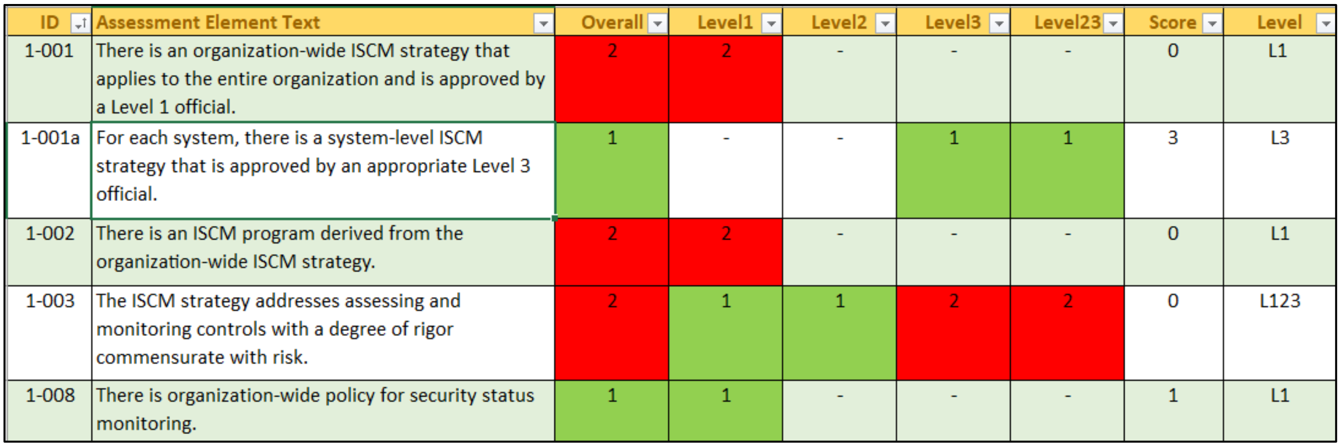
The *MasterAssessment* worksheet, the Level worksheets, and the *JudgmentTable* worksheet described in the remainder of this section contain numeric values that represent judgments. Since the number of judgments, N, is tailorable (see Section 5.3.1), each judgment is representable by its relative number (e.g., 1, 2, 3, …, N) in the list of judgments as they appear—left to right, strongest to weakest—on the assessment forms. In all cases, the value 1 represents the strongest judgment, and N represents the weakest judgment.

4.9 MasterAssessment Worksheet

The *MasterAssessment* worksheet shown in Figure 34 is the result of combining the *Level1*, *Level2*, and *Level3* worksheets. The worksheet has five separate judgment columns that contain relative judgment numbers as described in Section 4.8: *Overall*, *Level1*, *Level2*, *Level3,* and *Level23*. The *Overall* column is the result of applying the algorithm for obtaining a single judgment for each element across all levels , as discussed in Section 2.8.3, while the *Level23* column is the result of the intermediate step that combines Level 2 and Level 3 judgments. The *MasterAssessment* worksheet provides a consolidated overview of the judgments from all the levels and how they are resolved into an overall judgment for the organization.

Unlike an individual assessment form, which is oriented to a specific risk management level and contains only a partial list of elements, the *MasterAssessment* worksheet contains all of the elements for the assessment-specified depth and breadth parameters.

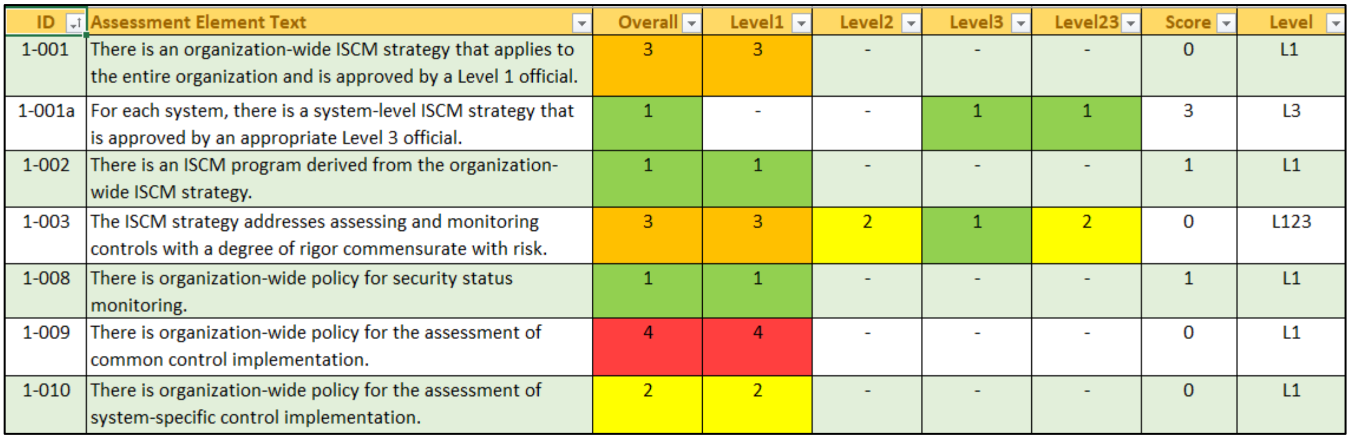
For recommended judgments, an example of the *MasterAssessment* worksheet is shown in Figure 33.



ID	Assessment Element Text	Overall	Level1	Level2	Level3	Level23	Score	Level
1-001	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	2	2	-	-	-	0	L1
1-001a	For each system, there is a system-level ISCM strategy that is approved by an appropriate Level 3 official.	1	-	-	1	1	3	L3
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	2	2	-	-	-	0	L1
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	2	1	1	2	2	0	L123
1-008	There is organization-wide policy for security status monitoring.	1	1	-	-	-	1	L1

Figure 33 - MasterAssessment Worksheet (Recommended Judgments)

For alternate judgments, an example of the *MasterAssessment* worksheet is shown in Figure 34.



ID	Assessment Element Text	Overall	Level1	Level2	Level3	Level23	Score	Level
1-001	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	3	3	-	-	-	0	L1
1-001a	For each system, there is a system-level ISCM strategy that is approved by an appropriate Level 3 official.	1	-	-	1	1	3	L3
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	1	1	-	-	-	1	L1
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	3	3	2	1	2	0	L123
1-008	There is organization-wide policy for security status monitoring.	1	1	-	-	-	1	L1
1-009	There is organization-wide policy for the assessment of common control implementation.	4	4	-	-	-	0	L1
1-010	There is organization-wide policy for the assessment of system-specific control implementation.	2	2	-	-	-	0	L1

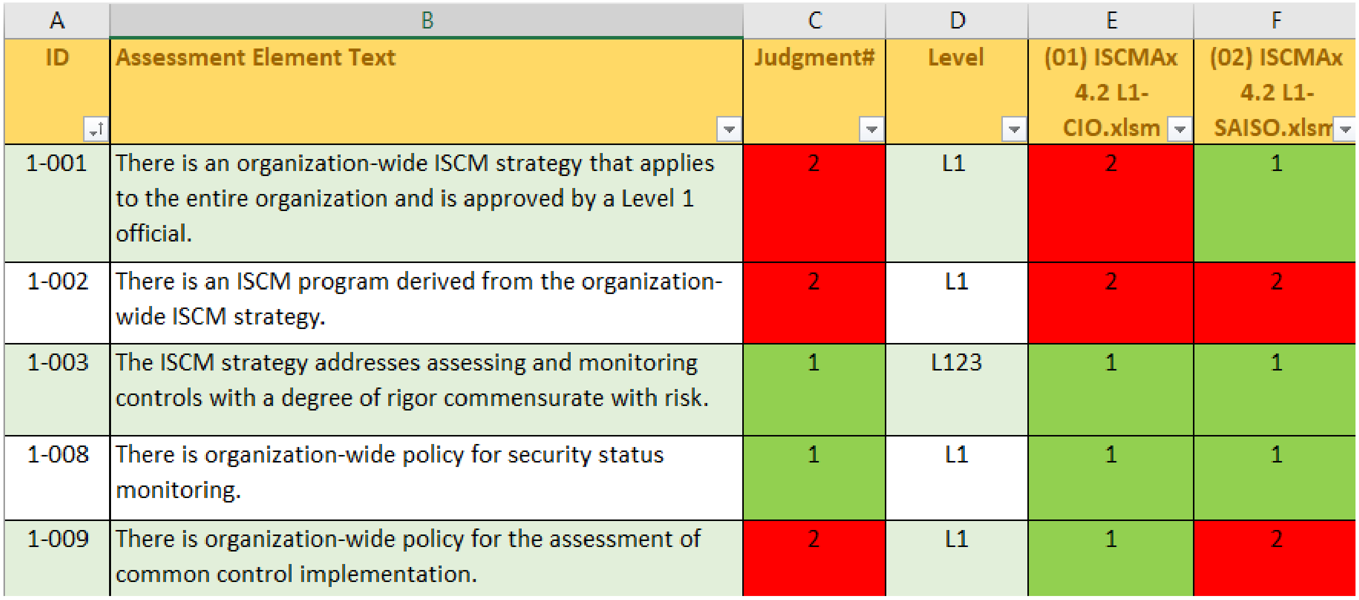
Figure 34 - MasterAssessment Worksheet (Alternate Judgments)

4.10 Level Worksheets

To consolidate scores, the merge process creates separate worksheets called *Level1*, *Level2*, and *Level3,* each of which consolidates all of the assessment files for the corresponding level. The *Level1*, *Level2*, and *Level3* worksheets each have one column for each individual assessment worksheet for the corresponding level. The values in each assessment worksheet column are the relative judgment numbers, as described in Section 4.8, from the corresponding assessment worksheet. The heading for each assessment worksheet column includes both the actual file name of each assessment worksheet from the working folder and a unique sequence number that is used in other worksheets as a short but unambiguous reference to the file name (columns E and F in Figure 35 below).

A consolidated judgment for a given level is obtained according to the resolution method—*majority judgment* or *weakest judgment*—determined in *Plan the Approach* (as described in Section 2.8.1).

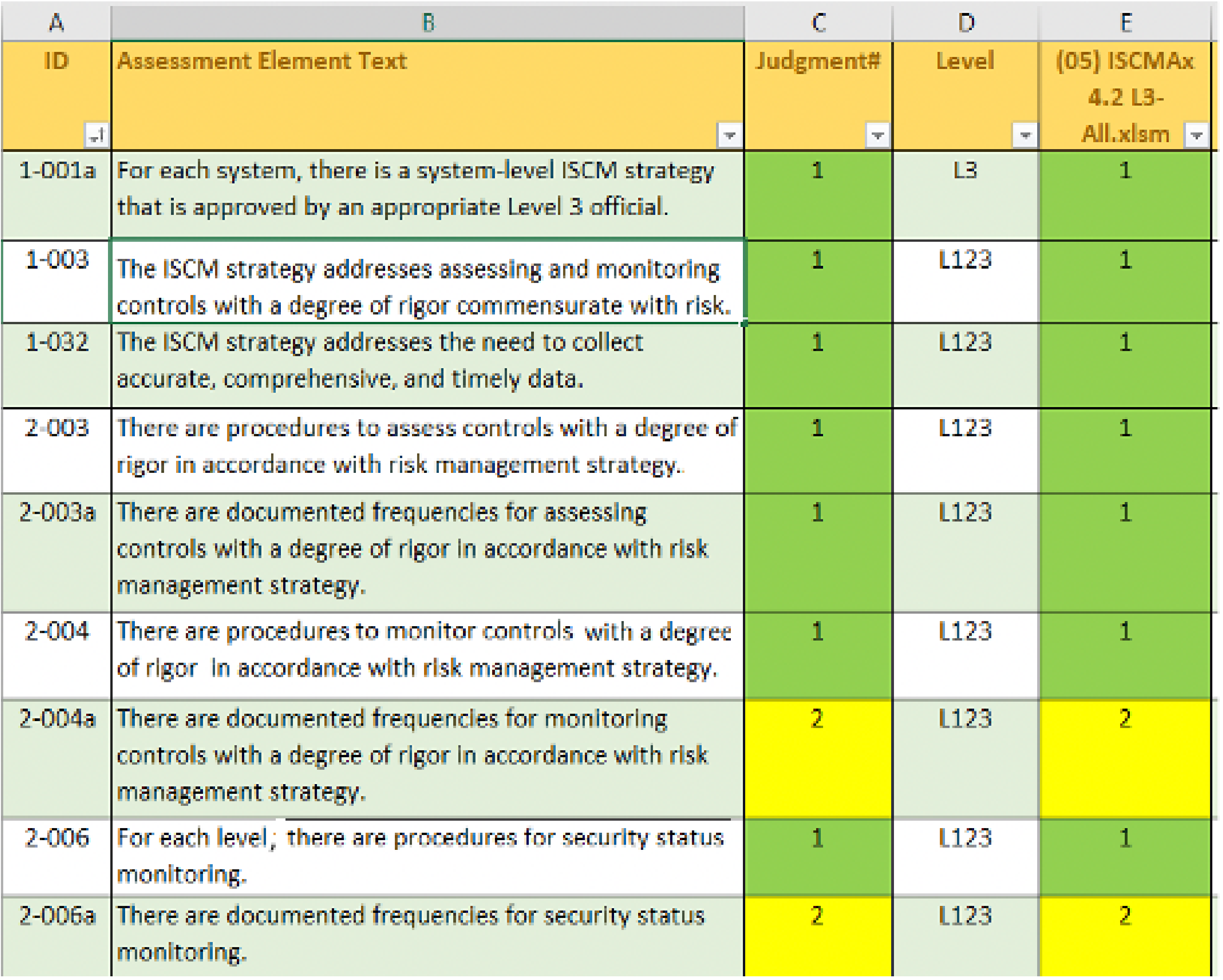
For recommended judgments, the *Level1* worksheet shown in Figure 35 shows that element 1-001 was judged 2 (*Other Than Satisfied*) in assessment worksheet (01) and 1 (*Satisfied*) in assessment worksheet (02) with the resultant judgment of 2 (*Other Than Satisfied*) in column C.



A	B	C	D	E	F
ID	Assessment Element Text	Judgment#	Level	(01) ISCMAx 4.2 L1-CIO.xlsm	(02) ISCMAx 4.2 L1-SAISO.xlsm
1-001	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	2	L1	2	1
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	2	L1	2	2
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	1	L123	1	1
1-008	There is organization-wide policy for security status monitoring.	1	L1	1	1
1-009	There is organization-wide policy for the assessment of common control implementation.	2	L1	1	2

Figure 35 - Level3 Worksheet (Recommended Judgments)

For alternate judgments, the *Level3* worksheet in Figure 36 shows that element 2-004a was judged 2 (*Somewhat True*) in assessment worksheet (05). The resultant judgment of 2 (*Somewhat True)* in Column C is identical to Column E because there is only one Level 3assessment worksheet.



A	B	C	D	E
ID	Assessment Element Text	Judgment#	Level	(05) ISCMAx 4.2 L3-All.xlsm
1-001a	For each system, there is a system-level ISCM strategy that is approved by an appropriate Level 3 official.	1	L3	1
1-003	The ISCM strategy addresses assessing and monitoring controls with a degree of rigor commensurate with risk.	1	L123	1
1-032	The ISCM strategy addresses the need to collect accurate, comprehensive, and timely data.	1	L123	1
2-003	There are procedures to assess controls with a degree of rigor in accordance with risk management strategy.	1	L123	1
2-003a	There are documented frequencies for assessing controls with a degree of rigor in accordance with risk management strategy.	1	L123	1
2-004	There are procedures to monitor controls with a degree of rigor in accordance with risk management strategy.	1	L123	1
2-004a	There are documented frequencies for monitoring controls with a degree of rigor in accordance with risk management strategy.	2	L123	2
2-006	For each level, there are procedures for security status monitoring.	1	L123	1
2-006a	There are documented frequencies for security status monitoring.	2	L123	2

Figure 36 – Level1 Worksheet (Alternate Judgments)

4.11 Chains Worksheet

A *chain* is a set of elements that represents a complete assessment concept. More precisely:

- There is exactly one element in the chain, called the *root*, that has no parent; and
- Every element whose parent is in the chain is also in the chain.

A chain can be visually represented as a tree-like structure based on the is-a-parent-of relationship. The root of the chain is shown on the far left in Figure 37. The chain display includes the following visual properties:

- The connecting lines represent the is-a-parent-of relationship.
- Each large box represents an assessment element and contains the element ID (top left corner), the overall judgment number (top center), and the element text.

- The upper right corner of each large box shows up to three smaller boxes containing the individual judgment numbers for the three risk management levels in order.
- Where a risk management level does not apply to the element, the symbol 🚫 appears instead of a small box.
- The color of the large box corresponds to the overall judgment for the element.
- The color of each small box corresponds to the judgment for its corresponding level.

Although chains are graphically represented in general in [SP800-137A], the chains produced by the merge process in [ISCMAx] include levels and judgments.

For recommended judgments, an example chain is shown in Figure 37.

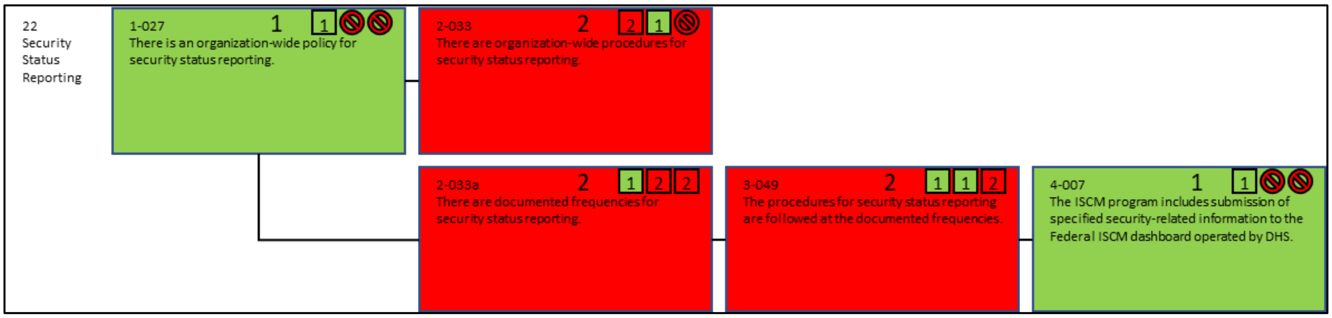

22
Security
Status
Reporting
1-027
1
1
There is an organization-wide policy for security status reporting.
2-033
2
2
1
There are organization-wide procedures for security status reporting.
2-033a
2
1
2
2
There are documented frequencies for security status reporting.
3-049
2
1
1
2
The procedures for security status reporting are followed at the documented frequencies.
4-007
1
1
The ISCM program includes submission of specified security-related information to the Federal ISCM dashboard operated by DHS.

Figure 37 - Chain (Recommended Judgments)

For alternate judgments, an example chain is shown in Figure 38

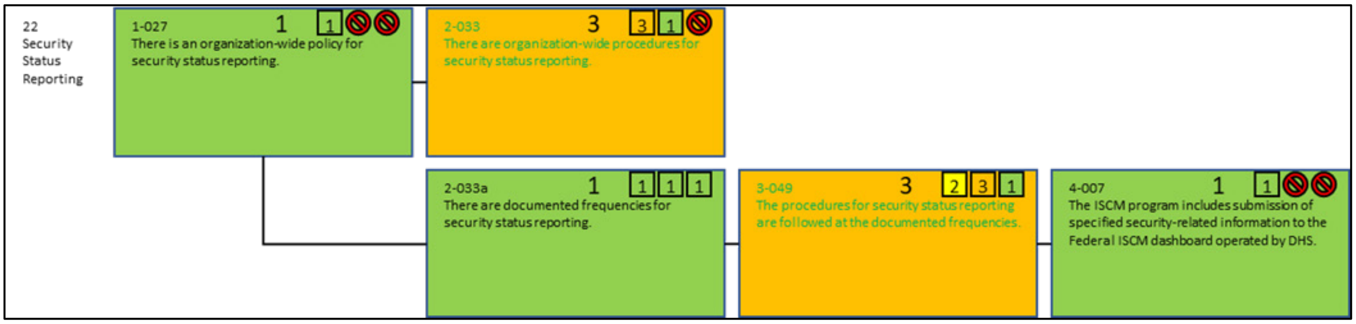

22
Security
Status
Reporting
1-027
1
1
There is an organization-wide policy for security status reporting.
2-033
3
3
1
There are organization-wide procedures for security status reporting.
2-033a
1
1
1
1
There are documented frequencies for security status reporting.
3-049
3
2
3
1
The procedures for security status reporting are followed at the documented frequencies.
4-007
1
1
The ISCM program includes submission of specified security-related information to the Federal ISCM dashboard operated by DHS.

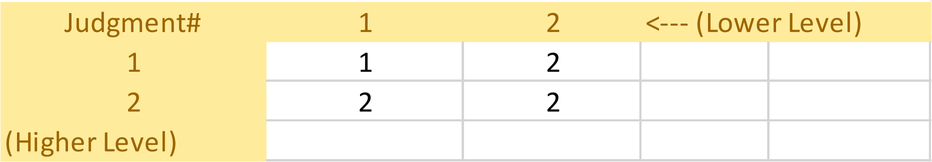
Figure 38 - Chain (Alternate Judgments)

Chains provide an additional way to organize and analyze the elements and associated scores that is independent of any reporting view. Each chain shows all the elements that address a single ISCM topic and its implementation across multiple ISCM process steps. For example, Figure 38 shows all of the elements that address Security Status Reporting.

4.12 JudgmentTable Worksheet

The *JudgmentTable* worksheet has the same structure as the table shown in Figure 6 (for recommended judgments) and Figure 7 (for alternate judgments) for obtaining a single judgment by combining judgments from two different risk management levels. All the numbers in Figure 39 and Figure 40 represent relative judgment numbers as described in Section 4.8. Judgments from all three levels are combined by first combining levels 2 and 3, then combining the result with Level 1.

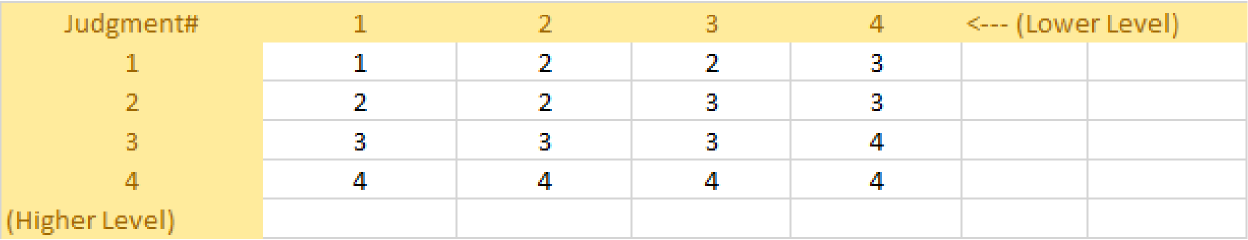
Figure 39 shows the judgment combination table for recommended judgments.



Judgment#	1	2	<--- (Lower Level)	
1	1	2		
2	2	2		
(Higher Level)				

Figure 39 - Judgment Combination Table (Recommended Judgments)

Figure 40 shows the judgment combination table for alternate judgments.



Judgment#	1	2	3	4	<--- (Lower Level)	
1	1	2	2	3		
2	2	2	3	3		
3	3	3	3	4		
4	4	4	4	4		
(Higher Level)						

Figure 40 - Judgment Combination Table (Alternate Judgments)

5 Tailoring

[ISCMAx] may be tailored to meet organization-specific needs. This section describes how tailoring is performed.

Tailoring is an organizational activity rather than a user activity. Because a single instance of ISCMAx operates at a single risk management level, there are at least three instances of ISCMAx involved in an organizational assessment (i.e., at least one instance for each risk management level). Each instance is an unmodified copy of the *post-tailoring* master template.

5.1 Tailoring the Elements

No [ISCMAx] element tailoring actions are performed on the Assessment worksheet. The organization does not directly modify the Assessment worksheet, which is programmatically derived from the Element worksheet and overwritten whenever the risk management level is changed. **Element tailoring is performed on the *Elements* worksheet**.

The *Elements* worksheet of an assessment file contains the key data underlying ISCMAx and is the source for all elements and associated attributes. To access the *Elements* worksheet for tailoring, click on the *Tailor Assessment* button in the far upper right of the assessment form. The *Elements* worksheet consists of the columns shown in Table 11.

1178 **Table 11 - Elements Worksheet**

Column	Description
ID	The element's unique identifier
Assessment Element Text	The full text of the element, representing an ISCM concept
Level	The risk management level(s) that evaluate the element (see Section 2.4)
Critical	A Yes/No value signifying that an element is of greater importance than non-critical elements; see [SP800-137A] for the criteria for this designation
Process Step	The process step associated with the element
Perspective	The value for the Perspective view
CSF Function	The value for the CSF Function view
CSF Category	The value for the CSF Category view
CSF.CAT	The value for the CSF.CAT view
Chain Label	The value for the descriptive label of the chain containing the element. The chain label is also used as the default presentation of the elements into sections during assessment
Parent	The element, if any, with the next higher process step that represents the same ISCM concept as the current element; both the element and its parent are part of the same chain.
Source	The source for this element (from [Catalog])
Assessment Procedure	The assessment procedure for this element (from [Catalog])
Discussion	Assistance and explanation to facilitate consistent evaluation of the element (from [Catalog])
Rationale for Level	Explanation of why a given element applies to one or more risk management levels.
Chain Sort	A key for sorting assessment elements so that they are grouped into chains and ordered by Process Step within the chain.

The actions available for tailoring elements are shown in Table 12.

Table 12 – Tailoring Actions for the Element Worksheet

Tailoring Action	ISCMAx Mechanism
Modify the text of an element	• Modify the *Assessment Element Text* value. If the change of the element text is significant, the change may be more appropriately made by adding a new element.
Modify one of an element's view mappings	• Modify the value in the appropriate view's column (Chain Label, Process Step, CSF Category, and Perspective). The values in each view's column are assumed to also appear in the view's row in the *Store* worksheet (see Section 5.2). The order of the values in *Store* determines the order in which they are displayed in assessment output.
Modify the discussion for an element	• Modify the value in the *Discussion* column. The guidance in the *Discussion* column is displayed during the assessment by clicking the *Notes*/*Help* icon (Figure 19) when making a judgment. • An example of an appropriate reason for tailoring the Discussion is to add organization-specific instructions for selecting specific judgments.
Modify the criticality of an element	• Modify the value in the *Critical* column. For a *detailed* assessment, changing the value in the *Critical* column changes the numeric weight for a given element and may affect the percentage score. Criticality has no effect on the percentage score of a *basic* assessment.
Add a new element	• Add a row giving appropriate values to each of the columns. **Do not duplicate an existing *ID***. It is recommended that any new *ID*s use a naming convention that distinguishes them from the ISCMA *ID*s. Names are limited to 12 characters. Any number, letter, or one of the characters "-" or "_" is valid.

Tailoring Action	ISCMAx Mechanism
Delete an element *Note: It is recommended that original ISCMA elements are **not** deleted. Element deletion is intended only for elements previously added by the organization.*	• Delete the row. If the element being deleted is the parent of other elements, the *Parent* columns for the other elements must be modified to point back to an appropriate parent for the *chains* functionality to operate properly.
Modify the level for an element	• Modify the value in the *Level* column. The value begins with the letter "L" and is followed, without spaces, by the risk management level(s) to which the element applies (e.g., L12).

5.2 Tailoring Views

Views are implemented in the *Store* worksheet in the section labeled "…Views." To access the *Store* worksheet for tailoring, click on the *Tailor Assessment* button in the far upper right of the assessment form. There is one row for each view and an additional row that lists all the views. The first view in the list of all views is known as the *primary* view and is the view used to organize the elements during the assessment. The ISCMAx default primary view is the *Section* view. [8] Other than by identifying the primary view, the order of the views in the view list affects only the position of the view's output in the *ScoreSummary* worksheet.

There is also a row for view *aliases*, which are used to provide alternate names on the radar charts, should this be desired.

Note that *Process Step* is listed as a view. While *Process Step* is a view in many respects, the *Process Step* view has a special role in ISCMA as the foundation of the ISCM process, and modifying individual process steps or deleting the *Process Step* view undermines the integrity of the ISCMAx application.

The actions available for tailoring views are shown in Table 13.

[8] *Section view* is used for whichever view is selected by the user to present the elements for assessment. In the example, Chain Label view is used, but ultimately, any view can be used, including views added by the user.

Table 13 - ISCMA View Tailoring Actions

Tailoring Action	ISCMAx Mechanism
Modifying which view is the primary view	In the *Store* worksheet: • Edit the *Primary View* row to the desired view.
Add a view	In the *Store* worksheet: • Insert a new list (row) directly under the last existing view. Beginning in column B, type the names of the view items. • Add the view name to the end of the list in the *Views* row. • Add an alias name (or "None") in the *ViewAliases* row. In the *Elements* worksheet: • Add a new column using the view name as the column header. • Populate the new column for all elements.
Delete a view	In the *Store* worksheet: • Delete the contents of the corresponding cell of the *Views* row. • Move the items after the gap one cell to the left to close up the list. Do not leave a gap in the list as view functionality will be affected. • Delete the old view's list (row) if desired (functionality not affected). • Delete the old view's column in the *Elements* worksheet if desired (functionality not affected).
Modify the items associated with a view	In the *Store* worksheet: • Modify the items in the view's defining row. In the *Elements* worksheet: • Modify the view's column for all elements as necessary to ensure that every value in the *Elements* worksheet is listed in the view's definition in the *Store* worksheet.

5.3 Tailoring Judgments

Tailoring the judgments that can be made about an element is the most complex tailoring action that can be made to ISCMAx. There are up to three separate tasks required to tailor judgments:

1. Tailoring the individual judgments themselves;
2. Tailoring the element-level guidance for making the judgments; and
3. Tailoring the table used to combine multiple judgments across risk management levels.

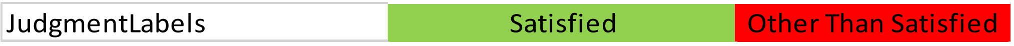
The tasks required to tailor judgments are addressed in the next three sub-sections, and an additional example of tailoring judgments is described in Section 5.6.

Judgments are tightly related to scoring, but judgments and scoring can be tailored independently to some extent. See Section 5.4 for a discussion of tailoring scoring.

5.3.1 Judgment Labels

The judgments that can be made about an element are stored as items in a list that is strongest at the beginning (left) and weakest at the end (right) with possible gradations between. The minimum number of judgments is two.

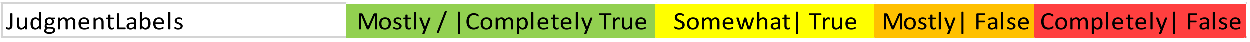
Figure 41 shows the recommended ISCMA judgment labels, as specified in [SP800-137A].



JudgmentLabels	Satisfied	Other Than Satisfied

Figure 41 - Judgment Configuration Parameters (Recommended Judgments)

Figure 42 shows the alternate ISCMA judgment labels.



JudgmentLabels	Mostly / |Completely True	Somewhat| True	Mostly| False	Completely| False

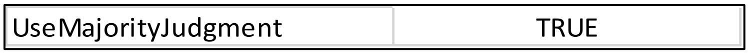
Figure 42 - Judgment Configuration Parameters (Alternate Judgments)

The judgment labels appear directly on the assessment form and the appropriate judgement is selected via a radio button. The vertical bar symbol (“|”) in a judgment label indicates a line break at that location in the label, which is useful for conserving horizontal real estate on the assessment form and allowing the user to control where breaks are in the longer tables. In any other use of these labels, this symbol is ignored.

A fill color is assigned to each judgment label and appears on the assessment form when a judgment is selected. The cells in the *Assessment* worksheets that store judgments are also filled with the assigned color.

5.3.2 Intra-Level Judgment Conflict Resolution

The configuration setting that determines how multiple judgments at the same risk management level are consolidated is the *UseMajorityJudgment* setting found in the section labeled Judgments & Scoring in the *Store* worksheet, shown in Figure 43. A setting of TRUE indicates the use of the Majority Judgment rule, while a setting of FALSE indicates the use of the Weakest Judgment rule. The judgment rules are described in detail in Section 2.8.1.



UseMajorityJudgment	TRUE

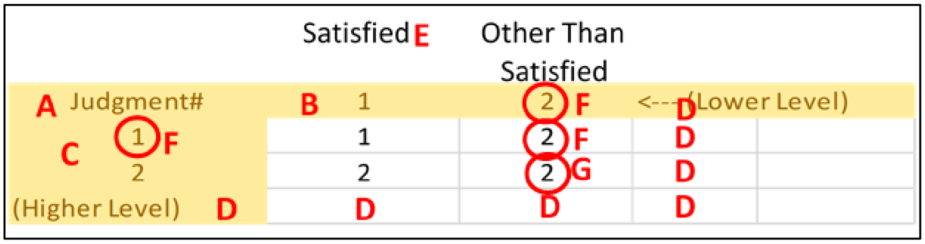
Figure 43 - Intra-Level Judgment Conflict Resolution Setting

5.3.3 The Judgment Combination Table

The table used to combine inter-level judgments is stored in the *JudgmentTable* worksheet. The judgment combination table is used only during the merge process, where risk management levels are combined to obtain a single overall judgment for each element.

The judgment combination table is constructed and modified by direct manual input into the cells of the *JudgmentTable* worksheet. The table satisfies the following list of [ISCMAx] requirements. Each item in the list is labeled with a letter that corresponds to a letter position in Figure 44 (recommended judgments) or Figure 45 (alternate judgments).

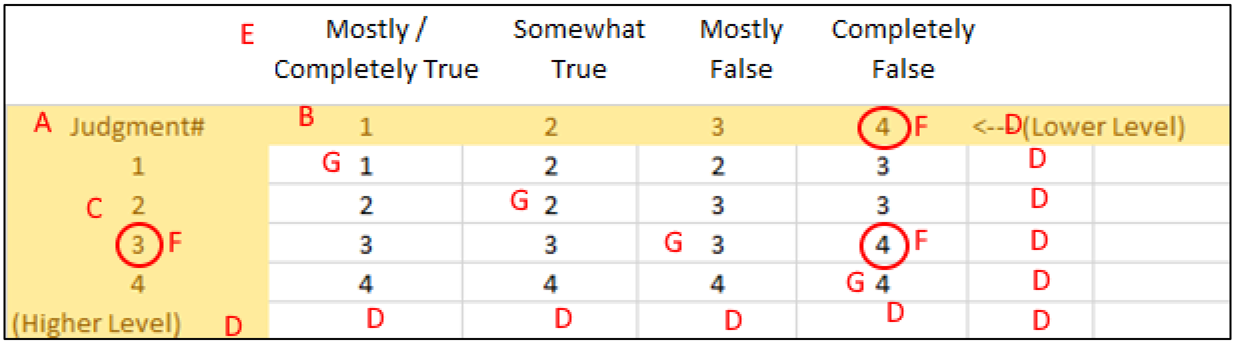
A. The table has a unique cell containing the word "Judgment#." The Judgment# cell is referred to as the *base* cell.
B. Immediately to the right of the base cell is the row of all relative judgment numbers (see Section 4.8) 1, 2, …, N, where N is the number of judgments. The values locate the judgment for the *lower*[9] level and are used to identify the columns of the table.
C. Immediately below the base cell is a column of relative judgment numbers 1, 2, …, N. These values locate the judgment for the *higher* level and are used to identify the rows of the table.
D. Any cells other than the $(N+1)^2$ cells bounded by the cells defined above are ignored.
E. The order of the judgment numbers corresponds to the order in the judgment list in the *Store* worksheet.
F. The value in any cell is the desired judgment number resulting from combining the higher level judgment (row label) with the lower level judgment (column label). This corresponds with Figure 6, Inter-Level Consolidation (Recommended Judgements).
G. For any cell on the diagonal, the value is the same as the row label/column label. That is, if the inputs are the same, then the result is the same as the inputs. This corresponds with Figure 7, Inter-Level Consolidation (Alternative Judgements).



	Satisfied	Other Than Satisfied		
Judgment#	1	2	<---(Lower Level)	
1	1	2		
2	2	2		
(Higher Level)				

Figure 44 - Judgment Combination Table Details (Recommended Judgments)

[9] The term *lower* refers to the structure of the organizational risk management level pyramid (i.e., Level 3 (System Level) is the lowest level).



E	Mostly / Completely True	Somewhat True	Mostly False	Completely False	
A Judgment#	B 1	2	3	4 F	<--D(Lower Level)
1	G 1	2	2	3	D
C 2	2	G 2	3	3	D
3 F	3	3	G 3	4 F	D
4	4	4	4	G 4	D
(Higher Level) D	D	D	D	D	D

Figure 45 - Judgment Combination Table Details (Alternate Judgments)

There is no requirement that the table be symmetric. In the example in Figure 45, combining row 3 (*Mostly False*) and column 1 (*Mostly/Completely True*) yields a 3 (*Mostly False*), while combining row 1 (*Mostly/Completely True*) and column 3 (Mostly False) yields a 2 (Somewhat True), which indicates that the judgment combination table in Figure 45 includes the following conflict resolution rules:

- If the higher level judgment is *Mostly False* and the lower level judgment is *Mostly/Completely True*, the result is *Mostly False*.
- If the higher level judgment is *Mostly/Completely True* and the lower level judgment is *Mostly False*, the result is *Somewhat True*.

5.3.4 Summary of Judgment Tailoring Actions

A summary of all judgment tailoring actions is shown in Table 14.

Table 14 - Judgment Tailoring Actions

Tailoring Action	ISCMAx Implementation
Modify judgment text	In the Store worksheet: • Edit the cells in the JudgmentLabels row.
Modify judgment colors	In the Store worksheet: • Modify the fill colors of the cells in the JudgmentLabels row.
Add a new judgment	In the Store worksheet: • Edit the JudgmentLabels row. • Correspondingly edit the ScoringValues row (see Section 5.4).
Delete a judgment	In the Store worksheet: • Delete the appropriate cell in the list labeled JudgmentLabels. Move any remaining judgments to the left as necessary so that there is no gap in the list. • Perform the corresponding action(s) in the ScoringValues row (see Section 5.4).
Choose the intra-level conflict resolution algorithm	In the Store worksheet: • Edit the UseMajorityJudgment row. Write TRUE to use the majority judgment algorithm. Write FALSE to use the weakest judgment algorithm.
Modify the judgment combination Table	In the JudgmentTable worksheet: • Edit the table cells, ensuring that the requirements shown in 5.3.3 are met.

5.4 Tailoring Scoring

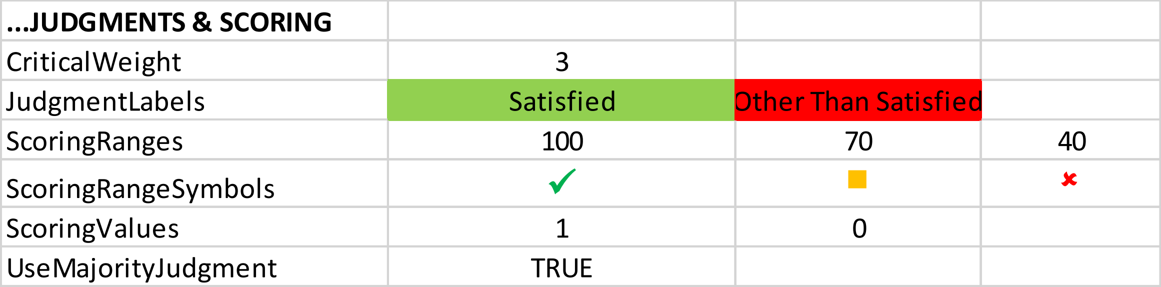
Scoring is based on the rows in the *Store* worksheet, as shown in Figure 46 (recommended judgments) and Figure 47 (alternate judgments), which contain the entire set of *Judgments and Scoring* tailoring options. The options which have not already been described in Section 5.3 are:

a) *ScoringValues*, a row of numeric values corresponding to the judgments in the *JudgmentLabels* row. The values are in non-increasing order, left to right. The first value represents the strongest judgment and is always 1.0. The last value represents the weakest judgment and is always 0.0. The number of *ScoringValues* in this list is the same as the number of *JudgmentLabels*.

b) *CriticalWeight*, the value used as a weighting factor for the scores of critical elements. Non-critical elements are assumed to have a weight of 1.0, and *CriticalWeight* is assumed to be ≥ 1.0. The default *CriticalWeight* for ISCMA is 3.0.

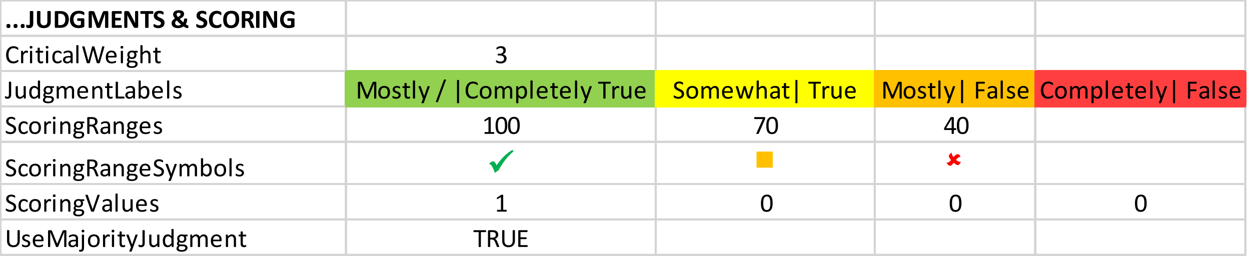
c) *ScoringRanges*, a row of numeric values that are used to group scores. The values represent the highest values of ranges. The number of *ScoringRanges* is independent of the number of *JudgmentLabels*. The *ScoringRanges* are used in the graphical output radar charts shown in Figure and Figure 27.

d) *ScoringRangeSymbols,* a row of symbols used to indicate both points on radar charts and colors for the associated *ScoringRanges*. The number of symbols matches the number of *ScoringRanges.* The symbols can be from any alphabet and will appear on radar charts exactly as they look in the *Store* worksheet. Note that, if desired, *ScoringRangeSymbols* can be used for letter grades, using the symbols "A," "B," etc. The font color of the symbols also determines the colors used in the summary scores bar shown in Figure 26.



...JUDGMENTS & SCORING			
CriticalWeight	3		
JudgmentLabels	Satisfied	Other Than Satisfied	
ScoringRanges	100	70	40
ScoringRangeSymbols	✓	■	✖
ScoringValues	1	0	
UseMajorityJudgment	TRUE		

Figure 46 - Judgments and Scoring Tailoring (Recommended Judgments)



...JUDGMENTS & SCORING				
CriticalWeight	3			
JudgmentLabels	Mostly / |Completely True	Somewhat| True	Mostly| False	Completely| False
ScoringRanges	100	70	40	
ScoringRangeSymbols	✓	■	✖	
ScoringValues	1	0	0	0
UseMajorityJudgment	TRUE			

Figure 47 - Judgment and Scoring Tailoring (Alternate Judgments)

For example, the rows in Figure 46 and Figure 47 each state that:

- All scores x, 100 >= x > 70 are in the green range.
- All scores x, 70 >= x > 40 are in the yellow range.
- All scores x, 40 >= x >= 0 are in the red range.

Table 15 - ISCMA Scoring Tailoring Actions

Tailoring Action	ISCMAx Mechanism
Modify the scores for each judgment	In the *Store* worksheet: • Modify the values in the *ScoringValues* row
Modify the relative weight for critical vs. non-critical elements	In the *Store* worksheet: • Modify the value in the *CriticalWeight* row
Modify the scoring range values	In the *Store* worksheet: • Edit the cells in the *ScoringRanges* row
Modify the scoring range symbols	In the *Store* worksheet: • Edit the cells in the *ScoringRangeSymbols* row
Modify the scoring range colors	In the *Store* worksheet: • Modify the font colors of the symbols in the *ScoringRangeSymbols* row

5.5 Miscellaneous Tailoring

5.5.1 Tailoring the Instructions

The instructions that appear on the initial screen of the assessment form may be tailored by directly modifying the *Instructions* worksheet. Anything, even a picture, that appears in column A is visible on the assessment form when the *Instructions* button is clicked.

The boundaries may also be moved. If either boundary is moved such that scrolling of the assessment form is necessary to see all of the content, the form will exhibit scrollbar(s).

5.5.2 Tailoring Miscellaneous Behavior Configurations

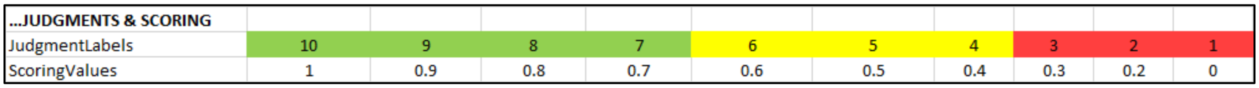
The following configuration items are available in the *Store* worksheet for unusual situations.

Table 16 - Miscellaneous Behavior Configuration

Configuration Item	Default Value	Description
AnswerRandomlyTargetScore	75	In the Excel View menu, the *AnswerRandomly* macro can be used to immediately fill the current assessment file with random judgments in order to achieve a specific target score. This may be useful in quickly creating examples for testing purposes. The assessment screen must be closed before running the macro.
ChainBoxShow	Assessment Element	This is the name of the column of the *Elements* worksheet whose value is shown on the element nodes in the Chains tab of the master worksheet.
ScrollWheelEnable	FALSE	This is an experimental feature that allows use of the mouse scroll wheel on the assessment form. Scroll wheel behavior is not automatically supported on Excel forms. If this value is FALSE, scrolling is achieved only by using the scroll bars. If this value is TRUE, the scroll wheel is enabled for element displays but will not always work on the *Completion* display.
ShowOverallScoreOnCharts	TRUE	This value can be set to FALSE to suppress the display of the overall score on radar charts in the master assessments.
ShowSheets	FALSE	If this value is TRUE, all sheets in the assessment file are unhidden. The same effect can be achieved temporarily by running the *ShowSheets* macro.

5.6 Example of Tailoring Judgments and Scoring

To allow judgments on a 1-10 scale, tailor the appropriate rows of the *Store* worksheet as shown in Figure 48.

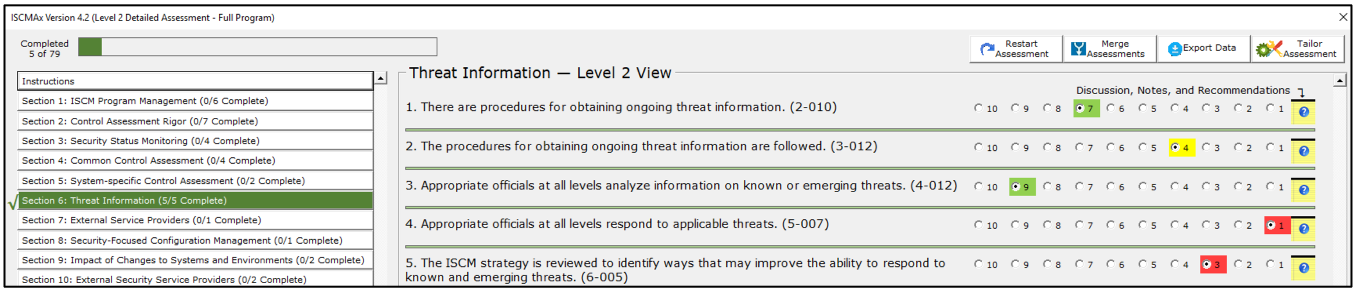


...JUDGMENTS & SCORING										
JudgmentLabels	10	9	8	7	6	5	4	3	2	1
ScoringValues	1	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0

Figure 48 - Configuring a 1-10 Scale

While 10 individual colors could be used here, three distinct colors—*green*, *yellow*, and *red*—are shown in Figure 48 to indicate a range. In addition, the scoring values chosen are uniformly decreasing (except at the end),) but this can be customized by the organization.

The 1-10 judgment scale appears on the assessment form as shown in Figure 49.



ISCMAx Version 4.2 (Level 2 Detailed Assessment - Full Program)

Completed 5 of 79

Instructions
Section 1: ISCM Program Management (0/6 Complete)
Section 2: Control Assessment Rigor (0/7 Complete)
Section 3: Security Status Monitoring (0/4 Complete)
Section 4: Common Control Assessment (0/4 Complete)
Section 5: System-specific Control Assessment (0/2 Complete)
✓ Section 6: Threat Information (5/5 Complete)
Section 7: External Service Providers (0/1 Complete)
Section 8: Security-Focused Configuration Management (0/1 Complete)
Section 9: Impact of Changes to Systems and Environments (0/2 Complete)
Section 10: External Security Service Providers (0/2 Complete)

Threat Information — Level 2 View

1. There are procedures for obtaining ongoing threat information. (2-010) ○ 10 ○ 9 ○ 8 ● 7 ○ 6 ○ 5 ○ 4 ○ 3 ○ 2 ○ 1

2. The procedures for obtaining ongoing threat information are followed. (3-012) ○ 10 ○ 9 ○ 8 ○ 7 ○ 6 ○ 5 ● 4 ○ 3 ○ 2 ○ 1

3. Appropriate officials at all levels analyze information on known or emerging threats. (4-012) ○ 10 ● 9 ○ 8 ○ 7 ○ 6 ○ 5 ○ 4 ○ 3 ○ 2 ○ 1

4. Appropriate officials at all levels respond to applicable threats. (5-007) ○ 10 ○ 9 ○ 8 ○ 7 ○ 6 ○ 5 ○ 4 ○ 3 ○ 2 ● 1

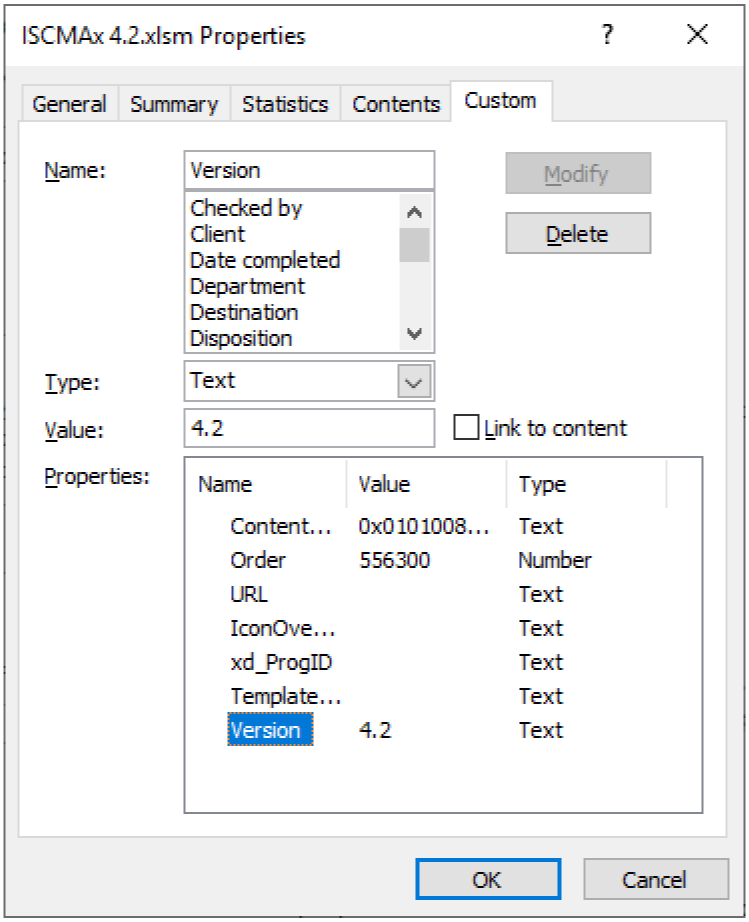
5. The ISCM strategy is reviewed to identify ways that may improve the ability to respond to known and emerging threats. (6-005) ○ 10 ○ 9 ○ 8 ○ 7 ○ 6 ○ 5 ○ 4 ● 3 ○ 2 ○ 1

Figure 49 - Using a 1-10 Scale

The scoring values shown demonstrate what is possible. However, regardless of the number of judgment labels, it is recommended that there be no partial scoring credit (i.e., that the strongest judgment label's scoring value be 1.0, and all remaining scoring values be 0.0).

5.7 The ISCMAx Version Identifier

The version identifier is displayed as part of the assessment form caption shown in Figure 16. The version identifier is a custom Excel document variable and is manually modified as part of the tailoring process. It is accessed from the Excel menu through *File\Properties\Advanced Properties*, which displays the dialog box in Figure 50.



Name: Version

Type: Text

Value: 4.2

Properties:

Name	Value	Type
Content...	0x0101008...	Text
Order	556300	Number
URL		Text
IconOve...		Text
xd_ProgID		Text
Template...		Text
Version	4.2	Text

Figure 50 - Modifying the ISCMAx Version Identifier

Type the new version identifier in the *Value* field. The version identifier can be replaced with any text, but it is recommended that the original version (4.0.4 in the example) be retained as a prefix (e.g., “4.0.4b Draft”) for traceability.

5.8 The Future of ISCMAx

[ISCMAx] is provided to the public as a reference implementation for the ISCMA methodology and is not intended to be a product that is enhanced by periodic updates. It is left to organizations, product vendors, or other interested parties to implement ISCMA with robust assessment products with additional features.

Appendix A—Glossary

Assessment element	A specific ISCM concept to be evaluated in the context of a specific Process Step
Base assessment	The ISCMAx assessment file from which a merge is initiated
Basic assessment	An assessment that includes only critical elements
Breadth	The steps of the ISCM process covered by an ISCM assessment: Strategy only (Step 1), Through Design (Steps 1, 2), Through implementation (Steps 1-3), or Full (Steps 1-6)
Chain	A set of elements that represents a complete assessment concept and are related by their *Parent* attribute
Depth	The amount of detail covered by an assessment: basic (both critical and non-critical elements) or detailed (all elements)
Detailed assessment	An assessment that contains all the elements (critical and non-critical) for a given breadth
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
External assessment engagement	Formal engagement led by a third-party assessment organization that determines element judgments
Facilitated self-assessment	Less formal than an internal assessment engagement, the element judgments determined by participant consensus on each element for a given level
Internal assessment engagement	Formal engagement led by a team within the organization that determines element judgments
Judgment	The association of an evaluation choice with an element, from the context of a specific risk management level
Level 1	The risk management level that addresses overall risk strategy, policies, and procedures for the entire organization. Also refers to any element that is meant to be evaluated by Level 1 personnel.
Level 2	The risk management level that addresses the risk strategy, policies, and procedures for a specific mission/business process (but not the entire organization). Also refers to any element that is meant to be evaluated by Level 2 personnel.
Level 3	The risk management level that implements ISCM for specific systems. Also refers to any element that is meant to be evaluated by Level 3 personnel.

Majority judgment algorithm

An inter-level judgment conflict resolution algorithm where the judgment that occurs most frequently is taken as the result. If more than one judgment occurs the greatest number of times, then the weakest such judgment is the result.

Process step

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

View

A classification of elements in which each element is associated with exactly one item of the classification

Weakest judgment algorithm

An inter-level judgment conflict resolution algorithm where the weakest judgment is taken as the result

Working folder

The Windows folder that contains all the ISCMAx assessment files to be merged into an organizational assessment

Appendix B—References

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

[CSF1.1] 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

[ISCMAx] National Institute of Standards and Technology (2020) *ISCMAx*. Available at https://csrc.nist.gov/publications/detail/nistir/8212/draft

[IGMetrics] *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1,* Department of Homeland Security, Washington, DC, May 2018. Available at https://www.dhs.gov/sites/default/files/publications/Final%20FY%202018%20IG%20FISMA%20Metrics%20v1.0.1.pdf

[SP800-37r2] 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

[SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-53, Revision 5. https://doi.org/10.6028/NIST.SP.800-53r5

[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

[SP800-137A] Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A