

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission.

Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM21-0340

Table of Contents

1	Introduction	6
1.1	Purpose of This Guide	6
1.2	Intended Audience	6
1.3	How to Use This Guide	6
1.4	Organization of the Guide	7
2	IRMPE Assessment Overview	8
2.1	IRMPE Assessment Process	8
2.2	IRMPE Assessment Architecture	8
2.3	Domain Descriptions	10
	Program Management (PM)	10
	Personnel and Training (PT)	10
	Data Collection and Analysis (CA)	10
2.4	MIL Scale	11
3	Conducting the IRMPE Assessment	14
3.1	Organizing for the Assessment	14
	Identifying the Scope of the Assessment	14
	Planning and Conducting the Insider Risk Self-Assessment	14
	Key Roles in the Assessment Process	14
	Meeting with the Sponsor and Other Stakeholders	15
	Suggestions for Meetings to Answer Assessment Questions	16
3.2	Completing the Assessment	17
	System Requirements and Setup	17
	Using the IRMPE Instrument	18
	Generating the Report	21
	Other Features of the Instrument	21
4	Interpreting the Insider Risk Self-Assessment Report	23
4.1	Insider Risk Self-Assessment Scoring	23
	Basic Rules	23
	Scoring Rubric	23
4.2	How to Interpret the Report	24
	Scores	24
4.3	Identify Gaps	26
5	Making Improvements	27
5.1	Analyze Identified Gaps	27
	Setting a Target: Method 1	28
	Setting a Target: Method 2	28
5.2	Prioritize and Plan	29
5.3	Implement Plans	29
6	Summary	30
	Appendix A: Process Checklist	31

Appendix B: Insider Risk Self-Assessment Glossary	33
Appendix C: References	39

List of Figures

Figure 1: The IRMPE Self-Assessment Domain Architecture	9
Figure 2: Organization Information	18
Figure 3: Example of Layout of Goals and Questions	19
Figure 4: Guidance Window	20
Figure 5: Notes Window	20
Figure 6: Example of Guidance and Notes Windows Opened at the Same Time	21
Figure 7: Instructions Page of the IRMPE Self-Assessment Instrument	22
Figure 8: Sample Performance Summary Page	24
Figure 9: Example of the Program Management Domain	25
Figure 10: Steps in a Typical Process Improvement Activity	26

List of Tables

Table 1: Insider Risk Self-Assessment Domain Composition	9
Table 2: Key Roles in the Assessment Process	14
Table 3: Instrument Buttons	19
Table 4: Insider Risk Self-Assessment in the Process Improvement Workflow	26
Table 5: Recommended Process for Using Results	27
Table 6: Insider Risk Self-Assessment Checklist	31

Notification

This document is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

1 Introduction

1.1 Purpose of This Guide

The purpose of this document is to enable organizations to conduct an Insider Risk Self-Assessment using an instrument designed for this purpose. The Insider Risk Self-Assessment instrument provides a measure of an organization's capabilities to operate and sustain an Insider Risk Program. This user guide:

- presents an overview of the IRMPE instrument structure and content
- provides information on how to prepare for an Insider Risk self-assessment
- provides information on how to conduct the assessment, which includes recording responses and scoring functions using the IRMPE instrument
- assists the organization in evaluating its Insider Risk Program capabilities
- provides guidance for follow-up activities

The Insider Risk Program Management Evaluation (IRMPE) methodology incorporates and expands on the cybersecurity concepts included in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). A crosswalk document that maps the methodology to the NIST CSF is included as a component of the IRMPE package of documents. The package also includes, this document, a Question Set and Guidance, and a Self-Assessment Quick Start Guide for expediting the self-assessment process.

The results of a self-assessment of an organization's Insider Risk Program represent an organization's capabilities only at a single point in time—at the time of the assessment. Even though certain aspects and questions in the Insider Risk Self-Assessment instrument are designed to indicate the organization's ability to sustain an Insider Risk Program over time, the organization should not rely on the assessment results as a conclusive expression of the organization's future cybersecurity capability.

1.2 Intended Audience

This user guide is intended for use by the individual who plans to conduct an Insider Risk Self-Assessment. In this document, this individual is called the practitioner. Typically, the practitioner is accountable to a sponsor within the organization who has requested or agreed to an Insider Risk Self-Assessment.

1.3 How to Use This Guide

The practitioner should use this user guide as a starting point for preparing and executing the Insider Risk Self-Assessment. The practitioner should read through the entire guide and the supporting documents to become familiar with the IRMPE instrument, including the end-to-end process for conducting the assessment. Familiarity with these materials is important because each self-assessment is different and may require the practitioner to adapt the process and related discussion to the needs of the organization being assessed. Although the guide is intended to help ensure consistency of approach and data, there may be situations where some adjustments are necessary to ensure a successful and valuable outcome for the organization conducting the self-assessment.

1.4 Organization of the Guide

Section [2](#), [IRMPE Assessment Overview](#), describes the Insider Risk Self-Assessment architecture as well as the individual components that make up the assessment.

Sections 3 through 5 describe the three key phases of a typical assessment process:

- Section [3](#): [Conducting the IRMPE Assessment](#), describes how the organization prepares for the assessment, conducts the assessment, and completes the form in the instrument.
- Section [4](#): [Interpreting the Insider Risk Self-Assessment Report](#), describes how the results documented in the assessment report are interpreted within the context of the organization.
- Section [5](#): [Making Improvements](#), describes how the organization determines next steps for improving its Insider Risk Program management practices.

Section [6](#), Summary, provides a brief summary, followed by appendices including a process checklist, a glossary of terms used in this document, and a list of relevant references.

2 IRMPE Assessment Overview

2.1 IRMPE Assessment Process

The Insider Risk Self-Assessment is a lightweight assessment method that was created by the Department of Homeland Security (DHS) for the purpose of evaluating an organization's Insider Risk posture. The Insider Risk Self-Assessment instrument consists of questions and guidance, and is designed to take approximately four hours to complete. However, because it is a self-assessment, the actual time necessary to complete the process may vary. A practitioner can answer the instrument's questions and review guidance alone or in conjunction with support from an organization's personnel in Cybersecurity, Operations, Physical Security, Human Resources, and others who may be knowledgeable about the organization's processes; these various constituencies of insider risk vary among organizations.

2.2 IRMPE Assessment Architecture

The Insider Risk Self-Assessment is intended to assist organizations in identifying and addressing risk that originates from trusted insiders. Contemplating, and preparing for, unauthorized behavior by authorized personnel is a good first step to addressing the potential risk that insiders may pose to an organization. It is important for organizations to have a robust Insider Risk Program that can prevent, detect, and respond to insider threats.

This self-assessment instrument is intended to walk practitioners through the process of identifying their organizational strengths and weaknesses. The instrument focuses on the key elements of insider risk and supports practitioners in identifying and evaluating those elements. Because this is a self-assessment, organizations conduct the process alone. While there is no need for outside coaching or direction, organizations may reach out to third parties for support and clarification.

The instrument has been designed so that the entire process should take no more than four hours, although a single contiguous half-day of effort is not necessary to complete the process. Practitioners may find it helpful to organize support in the form of subject matter experts and to complete the instrument as a small team. It is also possible for a single practitioner with full knowledge of an organization's insider risk elements and status to complete the instrument independently and alone.

Table 1 summarizes the three domains of IRMPE: Program Management, Personnel and Training, and Data Collection and Analysis. The focus of IRMPE is on the cybersecurity risk posed to an organization by insiders, in particular where information communications and technology (ICT) are involved in delivering essential services. The three domains represent essential elements of an organization's Insider Risk Program. Additionally, an organization's ongoing success in deploying and operating an Insider Risk Program is contingent upon a clear understanding of both the program's current level of maturity and, as importantly, its potential target state for improved maturity. Maturity indicator levels (MILs) are used to help define those maturity states by measuring MIL practices according to a common scale.

Table 1: Insider Risk Self-Assessment Domain Composition

Insider Risk Self-Assessment Domain	No. of Goals	No. of Goal Practices
Program Management	5	24
Personnel and Training	7	12
Data Collection and Analysis	8	31
MIL Practices	4	39

Each domain is composed of a purpose statement and a set of specific goals and associated practice questions unique to that domain. The Assessment utilizes multiple sets of Maturity Indicator Level (MIL) questions, assigned to each goal. The MIL questions examine the institutionalization of practices within an organization.

Figure 1 presents graphically the Insider Risk Self-Assessment domain architecture. As shown in Table 1, the number of goals and practice questions varies by domain, and the set of MIL questions and the concepts they encompass are different for each of the three domains.

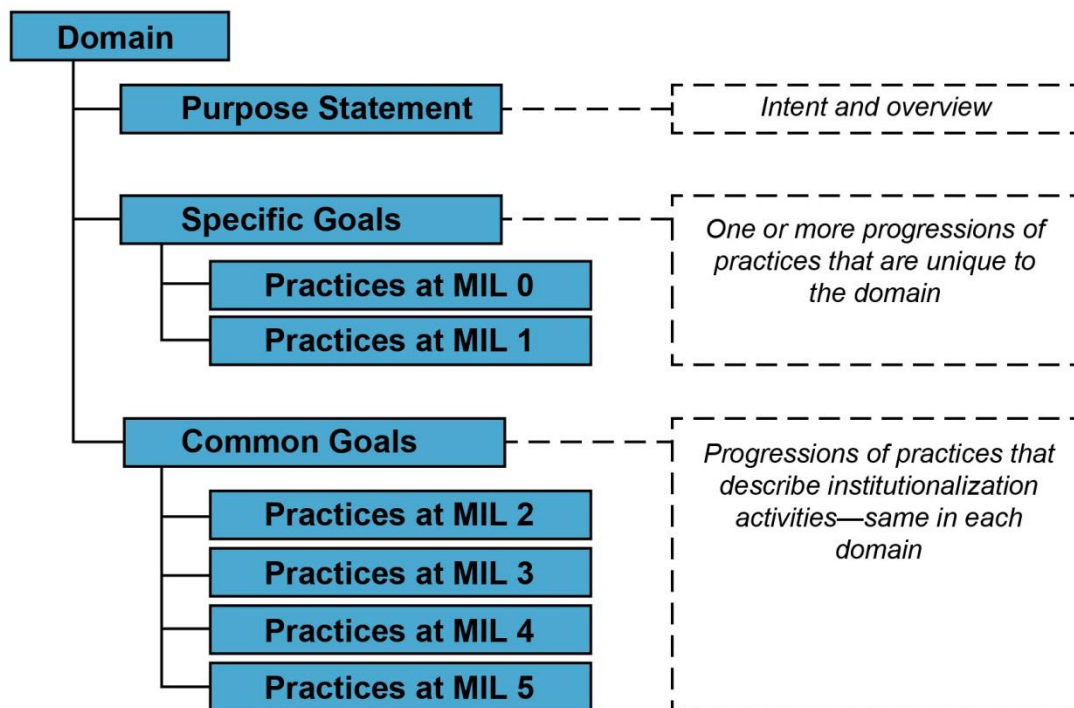


Figure 1: The IRMPE Self-Assessment Domain Architecture

2.3 Domain Descriptions

The following section describes the three Insider Risk Self-Assessment domains and MIL scale.

Program Management (PM)

The domain comprises five goals and 24 practice questions.

The purpose of the Program Management domain is to determine whether the organization has the management structures, policies, relationships, and communications in place needed as a foundation for an Insider Risk Program. Program Management includes the following:

1. understanding mission critical assets;
2. defining the Insider Risk policy for the organization;
3. characterizing the activities associated with insider threat prevention, detection and response;
4. ensuring communication of insider risk activities and events among responsible participants in the Insider Risk Program;
5. providing governance and oversight of insider risk activities; and
6. integrating insider risk management with organizational or enterprise risk management generally.

Personnel and Training (PT)

The domain comprises seven goals and 12 practice questions.

The purpose of the Personnel & Training domain is to determine if the organization has instituted the appropriate levels of insider risk awareness and training throughout the employee lifecycle. Personnel and Training includes

- insider risk awareness training for all personnel,
- role-based training for employees working with the Insider Risk Mitigation Team,
- role-based training for Insider Risk Mitigation Team members, and
- incorporation of insider risk training in the onboarding process.

Data Collection and Analysis (CA)

The domain comprises eight goals and 31 practice questions.

The purpose of the Data Collection and Analysis domain is to identify the elements and processes necessary to provide timely, accurate, complete, relevant, and actionable information about and response to an organization's insider risk environment. Key elements and processes include

- incident reporting,
- forensics and behavioral analytics,
- response mechanisms,
- time-focused actions,
- staff augmentation and organizational support, and
- other elements and procedures required to support an effective Insider Risk Program, both to align with an organization's standards and policy and to comply with relevant law and regulation.

2.4 MIL Scale

The Insider Risk Self-Assessment methodology uses maturity indicator levels to provide organizations with an approximation of the maturity of their practices in each of the three IRMPE domains. The Assessment's approach to maturity is based on an underlying capability maturity model, the CERT Resilience Management Model. In this approach, an organization's maturity is based on how completely the practices in each of the domains are institutionalized within the organization.

Institutionalization means that cybersecurity practices become a deeper, more lasting part of the organization because they are managed and supported in meaningful ways. When cybersecurity practices become more institutionalized—or embedded—managers can have a high degree of confidence in the practices' predictability and reliability. The practices also become more likely to be sustained during times of disruption or stress to the organization. Maturity can also lead to a tight alignment between cybersecurity activities and the organization's business drivers. For example, in more mature organizations, managers will provide oversight to a particular domain and evaluate the effectiveness of activities a domain comprises.

Example

The following example illustrates how MILs may be applied to the IRMPE's Program Management domain in a fictional organization.

Silicon Valley Healthcare Solutions (SVHS) provides a software service to providers of pharmaceuticals to the public: retail prescription drug stores, hospitals, clinics, and doctors. The SV-CareSol suite of products detects potentially unsafe drug interactions, alerts pharmacists of contraindications with existing medical conditions and allergies, and provides information to pharmacist consultation with the patient or customer.

Because SVHS tracks individuals' protected health information, it is subject to HIPAA privacy regulations and, as such, the company's Insider Risk Program is part of its core infrastructure support program. In particular, SVHS must ensure that the staff protects the confidentiality of healthcare information entrusted to them from either accidental or intentional compromise.

SVHS has a solid capability to prevent, detect, identify, assess, and manage insider events related to data confidentiality compromises. In particular, SVHS is currently at the insider risk self-assessment maturity level MIL2-Planned, meaning that there is a documented policy for performing the following activities, and stakeholders have been identified and made aware of their role in these activities:

- *Prevention, detection, investigation, and response to insider threat types identified as important to SVS, considering both positive and negative deterrence.*
- *Promoting the use of EAP to help employees with personal and professional stressors as needed.*

To move to a higher maturity level, SVS is implementing the following activities:

- *Oversight of program management functions and related risks, with periodic reviews and reporting of results to senior management*
- *Effectiveness of program management activities are measured and means for improvement implemented, as appropriate*
- *Dedicated and qualified staff supported by adequate funding of program management activities*

The expanded SVHS Insider Risk Program would be a first step towards a more mature program that exhibits behaviors associated with maturity level MIL4-Measured.

The MIL scale comprises six maturity levels, each with rigorous, defined components:

Incomplete → Performed → Planned → Managed → Measured → Defined

In the Insider Risk Self-Assessment process, a maturity level lower than Planned (MIL2) is considered to be incomplete, simplifying the maturity measurement process for Insider Risk Self-Assessment practitioners.

The six maturity levels for Insider Risk Self-Assessment are described below.

MIL0 Incomplete

Indicates that practices in an IRMPE domain are not being fully performed as measured by responses to the relevant domain questions.

MIL1 Performed

Indicates that all practices in an IRMPE domain are performed as measured by responses to the relevant domain questions. MIL-1 means that there is sufficient support for the existence of the practices.

MIL2 Planned

Indicates that a specific practice in an IRMPE domain is not only performed but is also supported by planning, stakeholders, and relevant standards and guidelines. A planned process or practice is

- established by the organization through policy and a documented plan
- supported by stakeholders
- supported by relevant standards and guidelines

MIL3 Managed

Indicates that all practices in an IRMPE domain are performed, planned, and have the basic governance infrastructure in place to support the process. A managed process or practice is

- governed by the organization
- appropriately staffed with qualified people
- adequately funded
- managed for risk

MIL4 Measured

Indicates that all practices in an IRMPE domain are performed, planned, managed, monitored, and controlled. A measured process or practice is

- periodically evaluated for effectiveness
- objectively evaluated against its practice description and plan
- periodically reviewed with higher level management

MIL5 Defined

Indicates that all practices in an IRMPE domain are planned, managed, measured, and consistent with all constituencies within an organization that have a vested interest in the performance of the practice. At MIL5, a process or practice is

- defined by the organization and tailored by individual operating units within the organization for their use
- supported by improvement information that is collected by and shared among operating units for the overall benefit of the organization

In the above progression, an organization can attain a given MIL only if it has attained all lower MILs. For example, an organization that fails to perform all MIL2 practices in a domain also fails to reach MIL3 in that domain, even if it has satisfied all the MIL3 requirements.

The IRMPE uses one maturity scale for all three domains because the domains represent different parts of a lifecycle—from establishing an Insider Risk Program to managing Insider Risk incidents and consequences—rather than representing a fundamentally different capability. Ideally, senior management should manage, measure, and oversee the organization's Insider Risk management capability throughout this complete lifecycle.

3 Conducting the IRMPE Assessment

3.1 Organizing for the Assessment

Identifying the Scope of the Assessment

Part of the practitioner’s role is to help the sponsor and the organization identify the scope of the assessment. There are three domains of assessment: Program Management, Personnel and Training, and Data Collection and Analysis. An assessment may be scoped to any combination of these three domains.

After the self-assessment scope is decided, planning can start.

Planning and Conducting the Insider Risk Self-Assessment

The Insider Risk Self-Assessment is completed by an individual practitioner or by a group with a practitioner leading the discussion. During the course of the assessment, the practitioner reviews each of the instrument’s questions and, either alone or with the group’s consensus, develops an answer for each. Participants in the groups may be drawn from various subject matter experts who can provide insight relevant to the IRMPE domains and program elements. The agreed-upon answer is then recorded in the assessment instrument before answering the next question.

The following section describes how to plan for and conduct an Insider Risk Self-Assessment. Sections [4](#) and [5](#) of this document provide guidance for interpreting the resulting report and planning follow-up improvement activities, respectively.

Key Roles in the Assessment Process

A successful Insider Risk Self-Assessment may require the active participation of members of the organization who serve in a variety of supporting roles. [Table 2](#) summarizes the key roles typically involved.

Table 2: Key Roles in the Assessment Process

Role	Description and Responsibilities
Sponsor	<p>The sponsor should have a broad understanding of the importance and components of an Insider Risk Program. General responsibilities include</p> <ul style="list-style-type: none"> • deciding whether the organization should conduct an Insider Risk Self-Assessment • selecting an individual to serve as the practitioner • ensuring that the resources necessary for the assessment are available • communicating the organization’s support for the assessment
Practitioner	<p>The practitioner is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the Insider Risk Self-Assessment. General responsibilities include</p> <ul style="list-style-type: none"> • delegating three domain leads, one for each self-assessment domains chosen during assessment scoping: Program Management, Personnel and Training, and Data Collection and Analysis • filling support roles, as needed • integrating the completion of the assessment instrument for each domain • generating the IRMPE report(s) • distributing the IRMPE report(s) to the sponsor and designees • assisting in the planning of follow-on activities

Role	Description and Responsibilities
Domain Leads	<p>The domain leads are identified, as necessary, and assigned by the practitioner to have overall responsibility for finding the answers to questions in the assigned IRMPE domains. General responsibilities include</p> <ul style="list-style-type: none"> identifying subject matter experts needed to answer questions for their domain meeting with subject matter experts to obtain question answers facilitating the completion of the assessment form in the instrument for their domain
Subject Matter Experts (SMEs)	<p>During the assessment, subject matter experts provide answers that best represent the organization's current insider risk capabilities in relation to the function or process being evaluated. It is most helpful for a SME to be</p> <ul style="list-style-type: none"> closely involved in the planning, implementation, or management of the domain represented able to represent organizational functions being assessed able to represent one or more of the organization's activities in the assessment's three domains

Meeting with the Sponsor and Other Stakeholders

Prior to conducting the self-assessment, the practitioner should meet with the sponsor, domain leads, and other stakeholders identified by the sponsor to prepare the organization for the assessment. The domain leads should familiarize themselves with the questions in their domain and think about strategies for answering them.

The objectives of this meeting include the following:

- Familiarize the sponsor, domain leads, and/or stakeholders with IRMPE.
- Discuss terms found in IRMPE that may differ from terms used within an organization, and ensure a common understanding.
- Obtain executive support and establish the role the sponsor wishes to play in the assessment.
- Identify the course of action for each assessment domain, with each domain lead in agreement (primary options identified below).
- Shape the stakeholders' expectations for the assessment (e.g., the phases of the process, required resources, personnel roles and responsibilities).
- Answer questions.

There are three primary courses of action (COA) that the group should agree to:

- COA1:** For each domain, the domain lead answers the questions for their domain, informally consulting SMEs they have access to on an as-needed basis. This COA may be preferred if the knowledge to answer the questions is largely available to the domain leads.
- COA2:** For each domain, the domain lead assembles a working group of SMEs to answer the domain questions. The domain lead organizes the group's logistics, i.e., whether to delegate the answering of subsets of the questions among the SMEs, or to have them meet to collaboratively answer the domain questions. This COA may be preferred if the knowledge to answer the questions is distributed throughout the organization, and if there is little overlap in the set of SMEs identified in the three domains.
- COA3:** The practitioner schedules one large meeting with all the SMEs identified by the domain leads to collaborate on answering the questions in all three domains. This COA may be preferred if the knowledge to answer the questions is distributed throughout the organization, but there is large overlap in the set of SMEs for the three domains.

Each domain lead is responsible for identifying the SMEs to be queried in order to answer the questions in their assigned domain.

When answering assessment questions, participants must consider practices as they are implemented currently. Do not consider activities that are planned or are in the process of implementation. Similarly, do not consider practices that have not been performed for extended periods of time. For example, if the organization has a user behavioral analytics process as part of its Insider Risk Program that the participants consider out of date to the point of being unusable, the process should not be considered.

Participants, or the practitioner alone, use a three-point response scale to evaluate the degree to which the organization has implemented each practice

- Yes – (fully implemented),
- No – (not implemented at all), or
- *Incomplete* – (partially implemented).

All participants should have a common understanding of when a particular response will be used.

Another point of discussion and agreement is a common understanding of how the assessment will be used within the organization's overall risk management program. The practitioner, with the support of the sponsor, should emphasize that next steps will be based on the organization's risks, resources, and maturity, and should point out the roles of participants in follow-up activities.

Suggestions for Meetings to Answer Assessment Questions

In collaboration with support staff, the practitioner should plan the entire process, including reserving a room large enough to accommodate all participants and assuring that the necessary computing hardware and software are available. See [System Requirements and Setup](#) in Section 3.2, for requirements for the instrument.

If the practitioner is assembling a team to conduct or support the self-assessment, it may be useful to begin with comments from senior management. Indeed, senior management support for the self-assessment process is essential to ensure that necessary resources and personnel are available to the process. An email from senior management to relevant organization personnel may be useful. Practitioner comments during process kick-off can help:

- emphasize the importance of IRMPE to the organization,
- identify the business drivers for the effort,
- emphasize the importance of managing internal risk, and
- highlight the importance of active participation of those who will support the initiative.

The practitioner should remind participants that the assessment is intended to provide a snapshot of the maturity and efficacy of the organization's insider risk management posture. Initiatives like IRMPE can provide a rare opportunity for discussion and teamwork among various departments, so it is worth reminding participants that they—not just the organization or the practitioner—can benefit from an honest and forthright discussion about the topics in the assessment. The practitioner should ensure that participants are prepared to contribute.

The following is advice for a successful process. It is understood that, because the instrument is a self-assessment, details about contributions, participants, and process are best defined by the

practitioner. In fact, in some situations, a practitioner may make an initial attempt at the instrument without other participation or contribution.

- A domain lead guides the participants through the assessment questions for the subject domain. Remember that open dialog and consensus-building are as important as the completed assessment.
- The practitioner enters answers into the instrument. It is preferred to have only one person who enters answers into the instrument.
- Some groups find it helpful to view a visual (projected) display of the assessment instrument. To begin, the domain lead shows participants the first questions from the domain and reads the description of the domain, the first goal, and the first question. The practitioner then describes the intent of the practice and reminds participants of the scoring guidelines.
- As the assessment progresses, it is helpful to display the questions and the responses participants have provided. The practitioner controls the responses recorded in the instrument and can display questions and responses as required. Notes regarding the discussions can also be reviewed to determine the rationale behind the responses given.

It is important to encourage discussion within the organization. There is value in allowing participants in the self-assessment to interact and discuss as a group what a consensus answer will be. The domain lead does not provide answers to the assessment questions but, rather, helps the group come to a consensus in its response. By facilitating the workshop, the domain lead helps the organization answer the assessment questions and formulate the next steps the organization must take when defining gaps and developing an improvement plan.

At all times, the practitioner is the lead for the process as a whole. The practitioner may need to remind participants not to get stuck on the specific phrasing of a question, but to focus on the intent behind the question. The assessment question guidance that is built in to the instrument can be useful in developing this understanding.

3.2 Completing the Assessment

The Insider Risk Self-Assessment Package consists of four PDF documents:

- Insider Risk Self-Assessment Instrument, a single Adobe PDF file titled “Insider Risk Mitigation Program Evaluation (IRMPE): Assessment Instrument”
- Insider Risk Self-Assessment Question Set And Guidance
- this IRMPE User Guide
- Insider Risk Self-Assessment Quick Start Guide

The Instrument facilitates

- a method for entering and recording answers
- automated scoring
- reporting with detailed results and suggested options for consideration

System Requirements and Setup

The instrument is designed to work with Adobe Acrobat X or higher, and may work with earlier versions of Adobe Acrobat. However, the file is unlikely to be viewable using third party applications.

JavaScript must be enabled in order for the instrument to work. JavaScript is enabled by default when Adobe Acrobat is installed.

The file is viewable using Adobe Reader. However, input to the instrument cannot be saved and data cannot be exported or imported using this free software.

The practitioner should save the document frequently to prevent potential data loss.

Using the IRMPE Instrument

The instrument enables simple input of assessment data by using text fields, dropdown boxes, and checkboxes. It begins with basic profile information about the practitioner and organization as shown in [Figure 2](#). The practitioner enters data by clicking any field, then typing the appropriate information. Press the **Tab** key or click another field to move the focus through the assessment.

Organization Information

*You **must** complete the Date of the Assessment field to be able to generate a report.
No other organization information is required to be entered on this page. These fields are provided for your internal use only.*

Facilitator

Name	<input type="text"/>
Title	<input type="text"/>
Phone <i>(Enter numbers only, no spaces or other characters)</i>	<input type="text"/>
Email	<input type="text"/>

Date of Assessment *(Please use popup calendar)*

Name of Organization

Business Unit/Agency

Organization Type *(Industry, Federal Entity, [SLTT](#))*

Sector

Physical Location

City	<input type="text"/>
State	<input type="text"/>

Figure 2: Organization Information

The assessment portion of the instrument is where the process begins. The IRMPE methodology and instrument focus on three domains as key elements of an Insider Risk Program.

- Project Management
- Personnel and Training
- Data Collection and Analysis

In the instrument, the practitioner selects a domain and a set of goals appear in a series, each goal comprised of a collection of questions. The practitioner reviews a question and then selects an answer from check boxes. Each question has three possible answers: *Yes*, *Incomplete*, and *No*. (See [Figure 3](#).)

- *Yes* – The organization fully performs the activity specified in the question.
- *Incomplete* – The organization partially performs the activity.
- *No* – The organization does not perform the activity at all.




Goal 1 - An Insider Risk policy exists.

The purpose of this goal is to ensure that the program has been established with the authority, scope, and responsibilities necessary to accomplish its mission.

		Yes	Incomplete	No	
1. Is there an authoritative document that establishes the existence of the Insider Risk Program?	G N	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	C
2. Does the authoritative document define the program's: - authority - scope - roles and responsibilities for stakeholders	G N	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	C

Figure 3: Example of Layout of Goals and Questions

Table 3: Instrument Buttons

Icon	Description and Action
	<p>Click the “G” button to open the Guidance window.</p> <p>The window includes a description of the intent of each question, the typical work products that could serve as evidence, and discrete criteria for <i>Yes</i> and <i>Incomplete</i> responses. (See Figure 4.) The Guidance window remains open until either the button is selected again or the Guidance window for a different question is opened.</p>
	<p>Click the “N” button to open the Notes window.</p> <p>The practitioner can dynamically enter notes related to that question, as shown in Figure 5. The Notes window will remain open until either the button is selected again, or the Notes window for a different question is opened. It is possible to have both the Guidance and Notes windows open at the same time as shown in Figure 6.</p>
	<p>Click the “C” button to clear the selection.</p>

Goal 1 - An Insider Risk policy exists.

The purpose of this goal is to ensure that the program has been established with the authority, scope, and responsibilities necessary to accomplish its mission. **Yes** **Incomplete** **No**

1. Is there an authoritative document that establishes the existence of the Insider Risk Program?

Question Intent: To determine if the Insider Risk Program was formally established in accordance with the organization's practices and procedures. Examples of authoritative documents include policies, directives, charters, or any other method by which the organization announces and establishes the existence of a program of record.

Typical Work Products:

- Policy
- Directive
- Charter
- Procedure

Criteria for "Yes" Response: The authoritative document formally established the Insider Risk Program in accordance with the organization's accepted practices.

Criteria for "Incomplete" Response: The authoritative document has been drafted, but has not been formally approved in accordance with the organization's accepted practices.

Notes:

Figure 6: Example of Guidance and Notes Windows Opened at the Same Time

Generating the Report

After all questions in the instrument have been answered, the practitioner can generate a report from the Instruction Page, which is provided at both the beginning and the end of the assessment section for convenience. As shown in [Figure 7](#), click **Generate Report** to create a report of the findings.

Important: Before you can generate a report in the Instruction Page, you **must** complete the **Date of Assessment** on the **Organization Page**. The other fields on the Organization Page are provided for your internal use only.

After the report is generated, you can select from two new options that appear on the Instruction Page: **Revise the Assessment** or **Print the Report**.

Note: The Instruction Page is located immediately before the report title page.

Other Features of the Instrument

- **Print Assessment** allows the practitioner to print the assessment tool, along with any checkboxes or other data that has been entered. This is *not* the same as the report of findings, which is produced by generating a report.
- **Export Data** allows the practitioner to save data from an assessment to an XML file.
- **Import Data** allows the practitioner to import a previous assessment using the data in an XML file that was exported previously by clicking **Export Data**.
- **Custom Data Import** allows the practitioner to import customized data that was exported previously to an XML file by clicking **Export Data**. The practitioner can import Organization Information data or any

or all data from the three IRMPE domains, Program Management, Personnel and Training, and Data Collection and Analysis.

- **Load Previous Responses** allows the practitioner to produce data for view from a previous self-assessment. A practitioner may find it useful to view previous self-assessment responses at the time when the current set of responses is entered into the instrument. Load Previous Responses also uses data from an XML file that was exported previously by clicking **Export Data**.
- **Clear Previous Responses** allows the practitioner to cancel **Load Previous Responses**.

PLEASE USE THE BUTTONS BELOW TO IMPORT AND EXPORT DATA, GENERATE THE REPORT, REVISE THE ASSESSMENT, PRINT THE REPORT, OR PRINT THE ASSESSMENT

Import Data
Export Data
Print Assessment
Generate Report

Include Facilitator Notes in the Report?
 Yes No

The buttons on this page are enabled based upon the state of your assessment and report.

- Initially, when in assessment mode, the **Import Data**, **Export Data**, **Print Assessment**, and **Generate Report** buttons are available.
- Upon selecting **Generate Report**, the **Generate Report** and **Print Assessment Form** buttons will change to **Revise Assessment** and **Print Report**, respectively. Once the report is generated, these buttons are now located directly above the report cover page.
- Upon selecting **Revise Assessment**, the **Revise Assessment** and **Print Report** buttons will change back to **Generate Report** and **Print Assessment Form**.
- Subsequent selections will toggle the document between displaying the assessment and displaying the report.

Generate Report – Performs assessment scoring and populates the report with all results. Facilitator Notes are not included by default, but may be included by changing the response to the Include Facilitator Notes question to 'Yes.' When the report is generated, the assessment portion of the document is hidden to prevent unintended changes as the document transitions to the report state. Once in the report state, you will see two new buttons:

Revise Assessment – Converts the document back to the assessment state, and hides the report which is no longer accurate until a subsequent report is generated.

Print Report – Prints the report.

Print Assessment – Prints the assessment.

Export Data – Allows a user to save data from the assessment in an XML file.

Import Data – Allows a user to import a previously completed assessment using an XML file that was exported using the **Export Data** button.

Custom Data Import - This feature allows a user to import only select sections of data exported from another copy of the Assessment. This also uses an XML file that was exported using the **Export Data** button.

Import Selected Sections

Organization Information
 Program Management
 Personnel and Training
 Data Collection and Analysis

Load Previous Responses - This feature allows a user to import their previous assessment responses in such a way that they can be viewed while a new set of responses is being recorded. This also uses an XML file that was exported using the **Export Data** button.

Load Previous Responses
Clear Previous Responses

Figure 7: Instructions Page of the IRMPE Self-Assessment Instrument

4 Interpreting the Insider Risk Self-Assessment Report

4.1 Insider Risk Self-Assessment Scoring

The scores for practice performance determine the scores for goal performance which, in turn, determine the final scoring result for each domain, expressed in the MIL scale. Scores of MIL2 through MIL5 indicate base practice performance as well as institutionalization of practices.

Basic Rules

1. Practices are either performed (the answer is *Yes*), incompletely performed (the answer is *Incomplete*), or not performed (the answer is *No*).
2. A goal is achieved only if all practices are performed.
3. A MIL1 score is achieved if all the goals in the three domains are achieved.
4. The domains can be achieved at higher levels if the MIL questions for each level (MIL2 through MIL5) are answered *Yes*.

Scoring Rubric

Step 1: Score the Practice Performances per Domain

Each practice in a domain is scored as follows:

- *performed* when the question is answered with a *Yes* (green)
- *not performed* when a question is answered with an *Incomplete* (yellow) or *No* (red) or *Not Answered* (gray)
- if *Not Answered* (gray) is shown, the question was left blank and is scored the same as a *No*.

Step 2: Score the Goal Achievement per Domain

Each goal within the domain is then scored as the following:

- *achieved* when all practices are performed (green)
- *partially achieved* when some practices are performed (yellow)
- *not achieved* when no practices are performed (red)

Step 3: Score the Maturity Indicator Level per Domain

Each domain is assigned a MIL based on the following:

- MIL0 if only some of the goals are achieved
- MIL1 if all of the goals are achieved
- MIL2 if MIL1 is achieved and all of the MIL2 questions are answered *Yes*
- MIL3 if MIL2 is achieved and all of the MIL3 questions are answered *Yes*
- MIL4 if MIL3 is achieved and all of the MIL4 questions are answered *Yes*
- MIL5 if MIL4 is achieved and all of the MIL5 questions are answered *Yes*

MILs are assigned to each domain and represent a consolidated view of performance. MILs describe attributes that would be indicative of mature capabilities as represented in the model's capability levels. However, MILs are not the same as capability levels.

4.2 How to Interpret the Report

Scores

The organization may use the Insider Risk Self-Assessment Report to create an action plan for addressing weaknesses and leveraging strengths identified in the assessment. A useful place to start is the IRMPE MIL 1-5 Performance Summary. [Figure 8](#) is an example of the summary for the Program Management domain.

Insider Risk Management Program Evaluation Report						MIL 1-5 Performance Summary				
IRMPE MIL 1-5 Performance Summary - Program Management						Table of Contents				
MIL-1 Performed:						MIL-2 Planned:	MIL-3: Managed:	MIL-4 Measured:	MIL-5 Defined:	
Domain practices are being performed.						Domain practices are supported by planning, policy, stakeholders, and standards.	Domain practices are supported by governance and adequate resources.	Domain practices are supported by measurement, monitoring, and executive oversight.	Domain practices are supported by enterprise standardization and analysis of lessons learned.	
Program Management	G1	G2	G3	G4	G5	1. Is there a plan for performing program management activities?	1. Is there oversight of the Insider Risk program?	1. Are program management activities periodically reviewed and measured to ensure they are effective and producing intended results?	1. Has the organization adopted a standard definition of program management activities from which operating units can derive practices that fit their unique operating circumstances?	
	1	1	1	1	1					
	2	2	2	2	2					
	3	3	3	3	3					
	4	4	4	4	4					
	5	5	5	5	5					
6	6	6	6	6						
2. Is there a documented policy for program management?						2. Have qualified staff been assigned to perform program management activities?	2. Are program management activities periodically reviewed to ensure they are adhering to the plan?	2. Are improvements to program management documented and shared across the organization?		
3. Have stakeholders for program management activities been identified and made aware of their roles?						3. Is there adequate funding to perform program management activities as planned?	3. Is higher-level management aware of issues related to the performance of program management?			
4. Have program management standards and guidelines been identified and implemented?						4. Are risks related to the performance of planned program management activities identified, analyzed, disposed of, monitored, and controlled?				

Legend

1(X) = Question Number (Subquestion Abbreviation)

- = Performed
- = Incompletely Performed
- = Not Performed
- S = Suppliers
- IP = Infrastructure Providers
- G = Governmental Services
- I = Information
- T = Technology
- F = Facilities
- P = People
- IM = Incident Management
- SC = Service Continuity

7 | IRMPE Assessment v 1.0

Figure 8: Sample Performance Summary Page

It is important to note that a higher maturity level can be achieved by an organization only if it satisfies all of the practices of all of the maturity levels below it. In other words, an organization that fails to perform all of the cybersecurity practices at MIL3 in a domain would also fail to reach MIL4 in that domain, even if it satisfied (answered Yes) all of the requirements at MIL4.

The MILs are an approximation of maturity in the organization. MILs describe attributes *indicative* of these capabilities if a more rigorous, formal appraisal process had found the same attributes. In other words, achieving a MIL does not necessarily imply an absolute capability in the sense of a formal appraisal, but it does *indicate* capability. The MIL scale is highly useful as an efficient way to focus on

improvement and to compare maturity across multiple domains. It is less useful as a rigorous, exact demonstration of a specific capability level in a single domain.

A performance summary may provide some initial insights into where to invest in cybersecurity improvements by drawing attention to the absence or weakness of practices performed.

The overview shows a linear display of an organization’s results. MIL1 reflects whether a goal has been fully achieved (green), has been partially achieved (yellow), or has not been achieved (red). For a goal to be fully achieved, all of the practices that make up the goal must be performed. MIL2 through MIL5 reflect whether each practice at a specific maturity level is performed (green), partially performed (yellow), or not performed (red).

A typical organizational objective may be to first achieve MIL2 in all domains and then, based on the organization’s risk tolerance, select other areas for improvement. An organization can use the overview to focus on prioritizing and implementing practices in the domains it chooses to improve.

Organizations should set their own path for improvement based on their organizational needs. For example:

- If an organization performs no practices in the Program Management domain, the organization should begin improvement in this domain first.
- If an organization has a regulatory compliance issue that is not being addressed and may result in a cost to the organization if not corrected, the organization may need to address practices related to that issue first. Regulations sometimes constrain an organization’s ability to employ a complete Insider Risk Program.

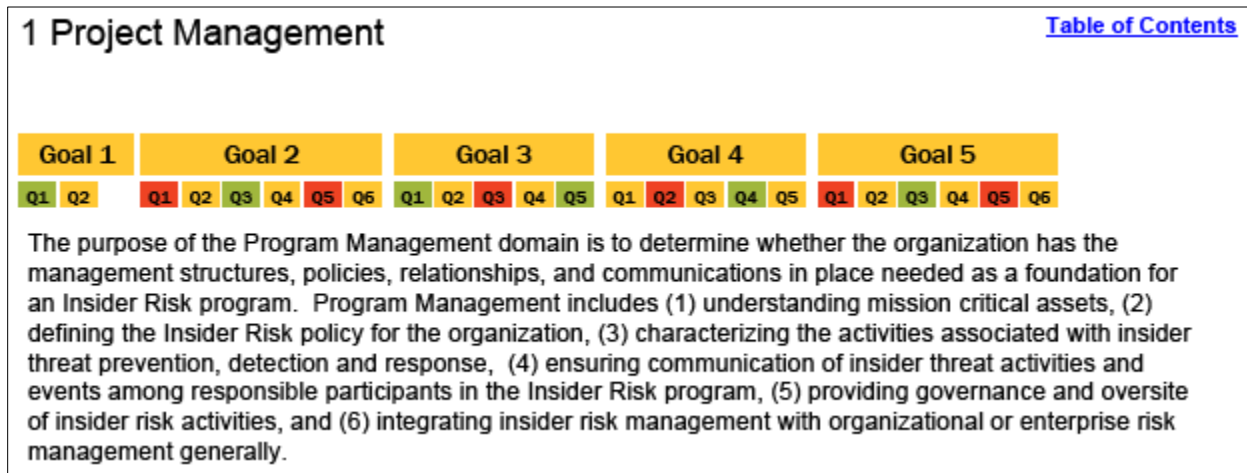


Figure 9: Example of the Program Management Domain

The Program Management Domain shown in [Figure 9](#) indicates that the organization may benefit from focusing on the prioritization, review, and requirements of the domain’s goals in order to advance from the current MIL2 to MIL3, because the organization is not yet performing all practices. The organization should focus on improvements in areas of highest risk, rather than simply try to achieve a higher MIL for its own sake.

4.3 Identify Gaps

IRMPE evaluates maturity across three domains and identifies specific gaps that can be used to initiate a process improvement project. A plan for improvement is guided in part by

- an evaluation of the assessment results;
- the identification of practice performance gaps in each domain;
- an alignment of each domain’s practices with the organization’s mission, strategic objectives; and
- the risk to critical processes and infrastructure, resulting in a target maturity level for each domain.

Figure 10 illustrates the iterative process of performing improvement activities.

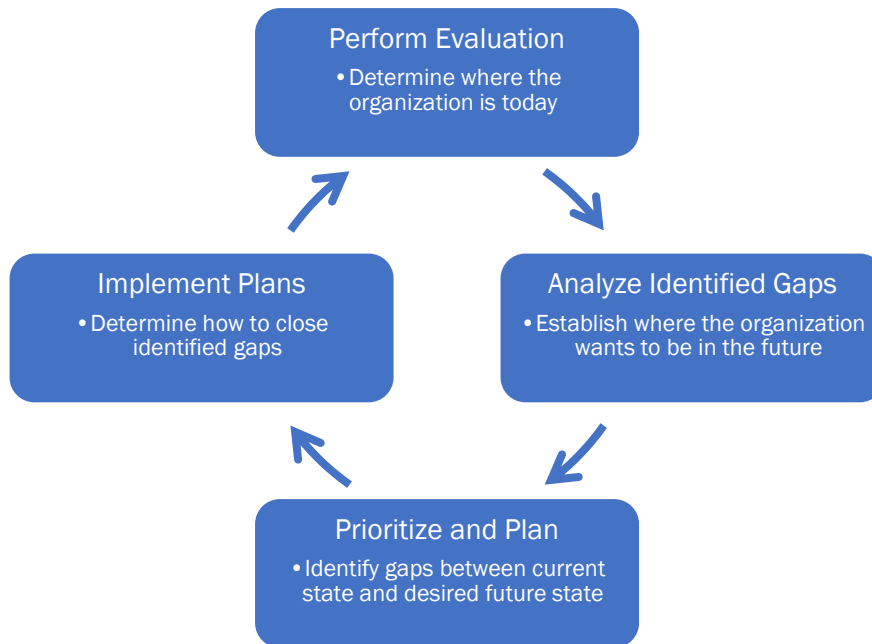


Figure 10: Steps in a Typical Process Improvement Activity

Table 4 shows the initial workflow for the process improvement activities.

Table 4: Insider Risk Self-Assessment in the Process Improvement Workflow

	Inputs	Activities	Outputs
Perform Evaluation	1. Insider Risk Self-Assessment previous results 2. Organizational policies and procedures 3. Understanding of current cybersecurity management and operations	1. Conduct the Insider Risk Self-Assessment	1. Insider Risk Self-Assessment Report

5 Making Improvements

The Insider Risk Self-Assessment does not prescribe the achievement of specific MILs for organizations in any particular critical sector. The report provides an organization, regardless of sector, with information on its current level of cybersecurity capabilities in each of the three IRMPE domains and can be used as a baseline for initiating a data-driven process improvement project, as depicted in [Table 5](#).

This section focuses on the three phases of a process improvement project that remain after the assessment is performed:

- Analyze Identified Gaps
- Prioritize and Plan
- Implement Plans

Table 5: Recommended Process for Using Results

	Inputs	Activities	Outputs
Analyze Identified Gaps	<ol style="list-style-type: none"> 1. Insider Risk Self-Assessment previous results, if available 2. Understanding the organization's objectives 	<ol style="list-style-type: none"> 1. Analyze gaps within the context of the organization (e.g., risk tolerance or risk profile) 2. Determine the potential impact of gaps to organizational objective 3. Determine which gaps should receive further attention 	<ol style="list-style-type: none"> 1. List of gaps and potential impact
Prioritize and Plan	<ol style="list-style-type: none"> 1. List of gaps and potential impact 2. Understanding of organizational constraints (e.g., resources, regulatory environment) 	<ol style="list-style-type: none"> 1. Identify potential actions to address gaps 2. Perform cost-benefit analysis for actions 3. Prioritize gaps and actions based on cost-benefit analysis and impact 4. Develop plan to implement prioritized actions 	<ol style="list-style-type: none"> 1. Prioritized implementation plan
Implement Plans	<ol style="list-style-type: none"> 1. Prioritized implementation plan 	<ol style="list-style-type: none"> 1. Monitor and measure implementation progress against plan 2. Reevaluate periodically and in response to major changes in the risk environment 	<ol style="list-style-type: none"> 1. Improvement plan tracking data

5.1 Analyze Identified Gaps

The Insider Risk Self-Assessment Report provides a detailed analysis, based on the responses recorded in the instrument. Summary charts show achievement of MILs by domain, and tables show the responses for each survey question. This data defines how well the organization scores against the criteria of IRMPE.

It may not be optimal for an organization to strive to achieve the highest MIL in all domains. The organization should, instead, determine the level of practice performance and MIL achievement for each domain that best enable it to meet its business objectives and cybersecurity strategy. This collection of desired capabilities is the organization's target state of practice performance and MIL achievement.

There are two common approaches for identifying a target state. The first approach, which involves using the results of the self-assessment to identify a desired target, is often adopted by organizations that are new to IRMPE and have not previously established targets. The second approach, which involves walking through practices before performing an assessment, is most typically adopted by organizations that have more experience and familiarity with IRMPE.

Setting a Target: Method 1

In this approach, a practitioner uses the results of a completed self-assessment to jump-start the identification of its target state. The organization begins by walking through its scores in each domain of the Self-Assessment Report and performing the following steps:

1. Identify all of the practices that have a *No* response.
2. For each practice that has a *No* response, review the practice and determine whether the practice must be performed to meet the organization's business and cybersecurity objectives.
3. If the practice must be performed, then document it.
4. If the practice does not need to be performed, then move to the next practice that had a *No* response.
5. Repeat steps 1 through 4 for all practices in the domain that have been identified as *Incomplete*.
6. Repeat for all three domains.

After this review is complete, the organization should have a documented list of practices that need to be performed. Combined with the list of practices the organization is performing already, which appears in the assessment report, the set of practices is the organization's target state of practice performance. One advantage of this approach is that the generated list of practices that need to be performed also serves as the list of gaps to be addressed. This list of gaps gives the organization a starting point for prioritizing and planning.

Setting a Target: Method 2

In this approach, a practitioner walks through IRMPE practices before conducting an assessment to identify its target state of practice performance and MIL achievement. The organization begins by walking through each of the practices in each domain, performing the following steps:

1. Review the practice and determine whether the practice must be performed to meet the organization's business and cybersecurity objectives.
2. If *Yes*, then document that practice.
3. If *No*, then move on to the next practice in the domain.
4. Repeat for all three domains.

After this review is completed, the organization will have a documented list of practices that it believes it must perform to meet its goals. This selection of practices is the organization's target state of practice performance, which then can be compared to the results of the assessment to determine where gaps exist that need to be addressed.

5.2 Prioritize and Plan

After the gap analysis is complete, the organization should prioritize the actions needed to fully implement the practices that enable the achievement of the desired capability in specific domains. The prioritization should be done using criteria such as:

- the effect of gaps on organizational objectives and critical processes and infrastructure;
- the criticality of the business objective supported by the domain;
- the cost of implementing the necessary practices; and
- the availability of resources to implement the practices.

A cost-benefit analysis for gaps and activities can inform the prioritization of necessary actions.

Next, the organization should develop a plan to address the selected gaps. Ideally, an organizational sponsor would be the owner of the plan, although responsibility for implementation may be assigned to a person designated by the sponsor.

5.3 Implement Plans

For the plan to succeed, organizations must provide adequate resources, including people with the necessary skills to accomplish the planned tasks and an adequate budget. In addition, the organization must continue supporting the execution of the plan by tracking progress and recognizing accomplishments.

After developing and implementing plans to address selected gaps, the organization should periodically reevaluate its business objectives and risks to determine if changes to desired capability are needed. Periodic re-assessment using IRMPE can track progress toward an organization's desired capability profile.

6 Summary

This document describes the IRMPE architecture and provides descriptions of the three Insider Risk Self-Assessment domains and maturity indicator levels (MILs). This document also contains information about how to prepare for an Insider Risk Self-Assessment and how a practitioner assists an organization in assessing the maturity of its cybersecurity capabilities. In addition, it provides guidance on follow-up activities to prioritize and implement a plan to close capability gaps that are identified through analysis of the Insider Risk Self-Assessment Report.

IRMPE also provides an assessment of an organization's capabilities relative to the NIST Cybersecurity Framework (CSF). Included in the IRMPE Package is a reference crosswalk that maps the relationship of NIST CSF categories and subcategories to Insider Risk Self-Assessment goals and practices.

For additional assistance, the practitioner and other participants can [contact the Department of Homeland Security \(DHS\)](#).

Appendix A: Process Checklist

The purpose of the IRMPE process checklist is to guide the Insider Risk Self-Assessment Process

Table 6: Insider Risk Self-Assessment Checklist

Item	Description	Completed												
Pre-Assessment														
Preparation Meeting	Hold a preparation meeting. <ul style="list-style-type: none"> • Answer organizational questions. • Establish the scope of the assessment. • Identify participants. • Schedule the assessment. 	<input type="checkbox"/>												
Facilities (as necessary)	Ensure that facilities have been set up correctly. <ul style="list-style-type: none"> • The room for the assessment is large enough to hold all participants and any observers, as necessary. • The room is set up to facilitate dialog among participants, as needed. • A projector and screen are available, if a group will be viewing the instrument. • One or more personal computers are available with Adobe Reader X or higher. Earlier versions of Adobe Reader may work. Third party applications will not work. 	<input type="checkbox"/>												
Availability	Confirm that all participants are available and committed to attend the workshop. <table border="1" data-bbox="479 1056 1300 1287"> <thead> <tr> <th>Name</th> <th>Title</th> <th>Role (Insider Risk Self-Assessment Domain)</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>Program Management (PM)</td> </tr> <tr> <td></td> <td></td> <td>Personnel and Training (PT)</td> </tr> <tr> <td></td> <td></td> <td>Data Collection and Analysis (CA)</td> </tr> </tbody> </table>	Name	Title	Role (Insider Risk Self-Assessment Domain)			Program Management (PM)			Personnel and Training (PT)			Data Collection and Analysis (CA)	<input type="checkbox"/>
Name	Title	Role (Insider Risk Self-Assessment Domain)												
		Program Management (PM)												
		Personnel and Training (PT)												
		Data Collection and Analysis (CA)												
Post-Assessment														
Interpret the IRMPE Report	Examine the IRMPE Report and answer the following questions: <ul style="list-style-type: none"> • What are the overall strengths and weaknesses (see the Overall Insider Risk Self-Assessment Results chart in the report)? <ul style="list-style-type: none"> ▪ What domains have not achieved at least MIL2? ▪ What domains have achieved MIL3 or above? ▪ What domains show the highest level of achievement? • What domain practices should the organization focus on (see the detailed domain sections of the report)? <ul style="list-style-type: none"> ▪ Identify the practices that are not performed at MIL2. ▪ Identify the MIL practices that are not performed at MIL2 in the domains that have achieved MIL2. 	<input type="checkbox"/>												

Item	Description	Completed
Analyze Gaps	<p>Determine where the organization wants to be and what the gaps are.</p> <ul style="list-style-type: none"> • Review each domain and identify what level of achievement is desired in the next three to five years. <ul style="list-style-type: none"> ▪ When identifying the target state, consider criteria such as the organization's business objectives and the criticality of the practice (or domain). • Compare the current state (the IRMPE Report) to the target state (where the organization wants to be in the next three to five years). <ul style="list-style-type: none"> ▪ Identify the practices that are not currently performed and are preventing the organization from achieving its target state. 	<input type="checkbox"/>
Prioritize and Plan	<ul style="list-style-type: none"> • Prioritize the practices not currently performed that must be performed to achieve the target state. Consider criteria such as <ul style="list-style-type: none"> ▪ how gaps affect organizational objectives ▪ the criticality of the business objective supported by the domain ▪ the cost of implementing the necessary practices ▪ the availability of resources to implement the practices • A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed. • Create a plan to achieve the target state, using the prioritized list of identified practices that must be implemented. 	<input type="checkbox"/>
Implement the Plan	<p>Implement the plan.</p> <ol style="list-style-type: none"> 1. Assign resources to implement the plan. 2. Periodically conduct self-assessments to measure progress. 3. Manage progress against the plan. 4. Re-plan as necessary. 	<input type="checkbox"/>

Appendix B: Insider Risk Self-Assessment Glossary

Term	Definition	Source
access	The ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge. National Industrial Security Program Operating Manual (NISPOM): The ability and opportunity to gain knowledge of classified information.	CDSE Glossary of Basic Insider Threat Definitions
analysis	The process by which information is transformed into intelligence; systemic examinations of information to identify significant facts, make judgments, and draw conclusions.	CDSE Glossary of Basic Insider Threat Definitions
asset	Person, structure, facility, information, material, or process that has value.	CDSE Glossary of Basic Insider Threat Definitions
awareness	Focusing the attention of, creating cognizance in, and acculturating people throughout the organization to resilience issues, concerns, policies, plans, and practices.	CERT-RMM
background screening	An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject.	CDSE Glossary of Basic Insider Threat Definitions
civil liberties	Rights granted to the people under the Constitution (and derived primarily from the First Amendment), to speak freely, think, assemble, organize, worship, or petition without government interference or restraints.	CDSE Glossary of Basic Insider Threat Definitions
controls	The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards.	CERT-RMM
counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.	CDSE Glossary of Basic Insider Threat Definitions
critical asset	A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.	CDSE Glossary of Basic Insider Threat Definitions
critical service	A set of activities an organization carries out in the performance of a duty or in the production of a product that is so critical to the organization's success that its disruption would severely impact continued operations or success in meeting the organization's mission.	CRR

Term	Definition	Source
cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.	CDSE Glossary of Basic Insider Threat Definitions
data collection & analysis (DC)	A domain of practice within the IRMPE. The purpose of the Data Collection and Analysis domain is to identify the elements and processes necessary for the purpose of providing timely, accurate, complete, relevant, and actionable information about and response to an organization's insider risk environment.	IRMPE
deterrence	The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.	CDSE Glossary of Basic Insider Threat Definitions
domain	In the context of the IRMPE structure, a domain is a logical grouping of cybersecurity practices that contribute to the cyber resilience of an organization.	IRMPE
enterprise	The largest (i.e., highest level) organizational entity to which the organization participating in the CRR survey belongs. For some participants, the organization taking the survey is the enterprise itself. See organization.	Adapted from SGMM v1.1 Glossary
event	One or more occurrences that affect organizational assets and have the potential to disrupt operations.	CERT-RMM
evidence	Testimonies, writings, material objects, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact. In the broadest sense, evidence consists of all matters that are logically relevant to the resolution of any issue of concern.	CDSE Glossary of Basic Insider Threat Definitions
facility	Any tangible and physical asset that is part of the organization's physical plant. Facilities include office buildings, warehouses, data centers, and other physical structures.	CERT-RMM
governance	An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT-RMM
human resources (HR)	The personnel within the workforce, including military officers and enlisted personnel (including members of the Reserve Components) and civilian employees working intelligence, counterintelligence, and security issues.	CDSE Glossary of Basic Insider Threat Definitions

Term	Definition	Source
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts.	Adapted from CERT-RMM
indicator	Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.	CDSE Glossary of Basic Insider Threat Definitions
insider	DoD Directive (DoDD) 5205.16: Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. NISPOM DoD 5220.22-M: Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems. EO 13587: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.	CDSE Glossary of Basic Insider Threat Definitions
Insider Risk Management Program or Insider Risk Program	A program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies.	EO 13587
insider threat (InT)	DoDD 5205.16: The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. NISPOM DoD 5220.22-M: The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information. EO 13587: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.	CDSE Glossary of Basic Insider Threat Definitions

Term	Definition	Source
law enforcement	The generic name for the activities of the agencies responsible for maintaining public order and enforcing the law, particularly the activities of preventing, detecting, and investigating crime and apprehending criminals.	CDSE Glossary of Basic Insider Threat Definitions
maturity indicator level (MIL)	The MIL scale measures the level of process institutionalization and describes attributes indicative of mature capabilities. Higher degrees of institutionalization translate to more stable processes that produce consistent results over time and that are retained during times of operational stress.	CRR
mitigation	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.	CDSE Glossary of Basic Insider Threat Definitions
monitoring	Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT-RMM (monitoring and risk management)
network	In critical infrastructure protection usage, a group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them.	CDSE Glossary of Basic Insider Threat Definitions
organization	An administrative structure in which people collectively manage one or more services as a whole and whose services share a senior manager and operate under the same policies. May consist of many organizations in many locations with different customers.	CERT-RMM
people	All staff, both internal and external to the organization, and all managers employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives.	CERT-RMM
Personnel & Training (PT)	A domain of practice within the IRMPE. The purpose of the Personnel and Training domain is to determine if the organization has instituted the appropriate levels of insider risk awareness and training throughout the employee lifecycle.	IRMPE
personnel security	The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.	CDSE Glossary of Basic Insider Threat Definitions

Term	Definition	Source
physical security	Security concerned with active, as well as passive measures, designed to deter intruders, prevent unauthorized access, including theft and damage, to assets such as personnel, equipment, installations, materials, and information, and to safeguard these assets against threats such as espionage, sabotage, terrorism, damage, and criminal activity.	CDSE Glossary of Basic Insider Threat Definitions
plan	A detailed formulation of a program of action.	Merriam-Webster
policy	A high-level, overall plan embracing the general goals and acceptable procedures of an organization.	Merriam-Webster
practice	An activity performed to support a domain goal.	CRR
Program Management (PM)	A domain of practice within the IRMPE. The purpose of the Program Management domain is to determine whether the organization has the management structures, policies, relationships, and communications in place needed as a foundation for an Insider Risk Program.	IRMPE
risk	A measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).	CDSE Glossary of Basic Insider Threat Definitions
risk assessment	Assessments that provide decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgements concerning the extent of actions needed to reduce risk. They provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessments generally include the tasks of identifying threats and vulnerabilities and determining consequences.	CDSE Glossary of Basic Insider Threat Definitions
risk mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.	CDSE Glossary of Basic Insider Threat Definitions
security	Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.	CDSE Glossary of Basic Insider Threat Definitions

Term	Definition	Source
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modeling and simulation) to support automated and/or human decision making (for example, concerning power system functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualization techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision making.	Adapted from SGMM v1.1 Glossary
stakeholder	A person or organization that has a vested interest in the organization or its activities.	CERT-RMM
technology asset	Any hardware, software, or firmware used by the organization in the delivery of services.	CERT-RMM
threat	An adversary having the intent, capability, and opportunity to cause loss or damage.	CDSE Glossary of Basic Insider Threat Definitions
threat analysis	A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.	CDSE Glossary of Basic Insider Threat Definitions
training	A set of activities that focuses on staff members learning the skills and knowledge needed to perform their roles and responsibilities in support of their organization's resilience program.	NIST SP 800-16
user activity monitoring (UAM)	The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threat and to support authorized investigations.	CDSE Glossary of Basic Insider Threat Definitions
vulnerability	Weakness in an information system, system security procedures, internal controls, physical or technical access controls, or implementation that could be exploited by a threat source; open to attack, harm, or damage.	CDSE Glossary of Basic Insider Threat Definitions

Appendix C: References

Center for Internet Security Controls, 2019, *CIS Controls, Version 7.1*. Retrieved August 12, 2021, from <https://www.cisecurity.org/controls/cis-controls-list/>

Office of the Director of National Intelligence, The White House, 2019, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Retrieved August 12, 2021, from https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

Software Engineering Institute, Carnegie Mellon University. 2016, *CERT Resilience Management Model (CERT-RMM), Version 1.2*, Retrieved August 12, 2021, from <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084>

Theis, M., Trzeciak, R., Costa, D., Moore, A., Miller, S., Cassidy, T., Claycomb, W., Software Engineering Institute, Carnegie Mellon University. 2019, *Common Sense Guide to Mitigating Insider Threats, Sixth Edition*, Retrieved August 12, 2021, from <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644>

U. S. Department of Commerce, National Institute of Standards and Technology, 2018, *NIST Cybersecurity Framework*, Retrieved August 12, 2021, from <https://www.nist.gov/cyberframework>

U. S. Department of Commerce, National Institute of Standards and Technology, 2019, *Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5*, Retrieved August 12, 2021, from <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

U. S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), 2020, *Cybersecurity Maturity Model Certification (CMMC), Version 1.02*, Retrieved August 12, 2021, from https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

