INSIDER RISK MANAGEMENT PROGRAM EVALUATION (IRMPE)

Quick Start Guide
Version 1.0

SEPTEMBER 2021

U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

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.

DM21-0340

Contents

List of Figures

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 document, 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 document.

DHS does not endorse any commercial product or service, including the subject of the analysis referred to in this document. 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 document 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 Getting Started

This Quick-Start Guide is designed to help you become familiar with the *Insider Risk Management Program Evaluation (IRMPE) Self-Assessment Instrument* to start your own IRMPE self-assessment. The tool is intended for use by the individual(s) who plan and coordinate the IRMPE within an organization.

Detailed guidance on how to use this tool is available in the *IRMPE User Guide.*

1.1 System Requirements and Setup

These are the system requirements to use the IRMPE Self-Assessment Tool:

- Adobe Acrobat X or higher; third-party applications are not compatible
- JavaScript enabled; JavaScript is enabled by default when Adobe Reader or Adobe Acrobat are installed.
- If you use the free version of Adobe Reader, you will not be able to save input to the tool, or import or export data.
- Save the tool frequently to prevent potential data loss.

1.2 User Interface

After you open the tool, and scroll past the copyright notice, to the Transition Page. You can perform the following actions in the Transition Page, as shown in Figure 1:

① Export data to an XML file.
② Import data from an XML file.
③ Print the assessment's questions and your answers.
④ Generate a report based on your answers to the questions (with option to include facilitator notes).
⑤ Import only selected portions from an XML file.
⑥ Load your answers from a previous year for comparison while filling out the tool this time.
⑦ Clear all of the responses to all of the questions entered so far in the tool.

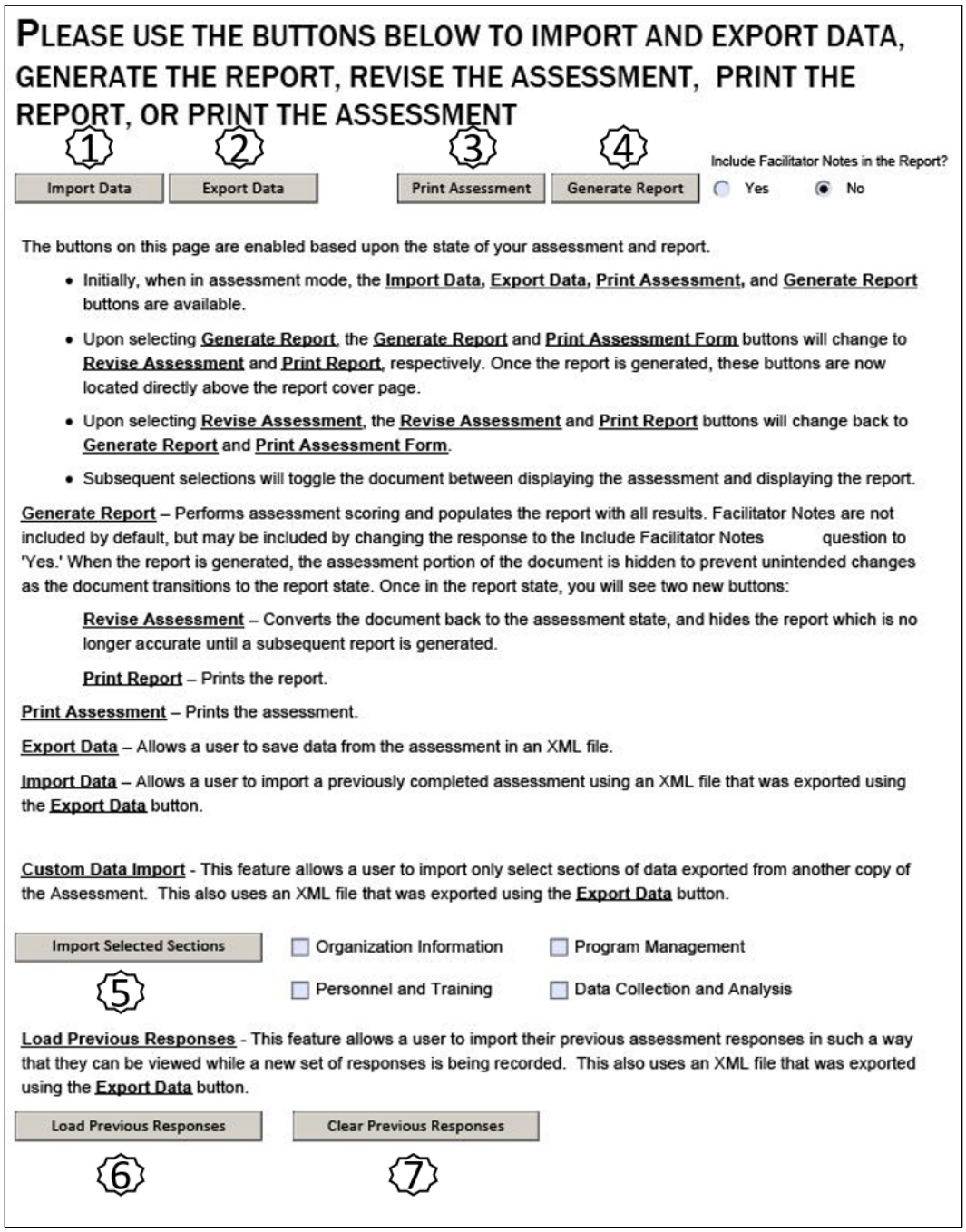

Figure 1: Transition Page

On the screen following the Transition Page is the Organization Information screen. You are not required to use these fields. All input is optional. However, if you want to generate a report, you must select a value in the **Date of the Assessment** field. **No other organization information** is required to be entered on this page. These fields are provided for your internal use only.

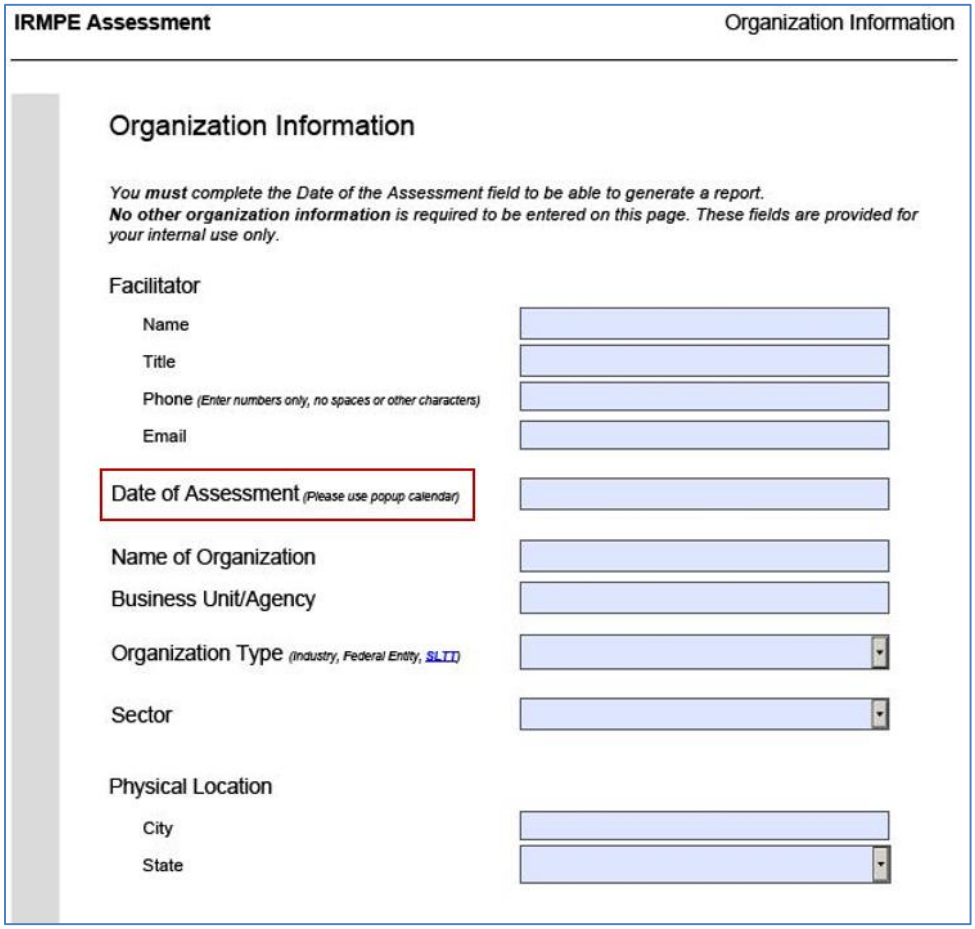

Figure 2: Date of Assessment Field in the Organization Information Screen

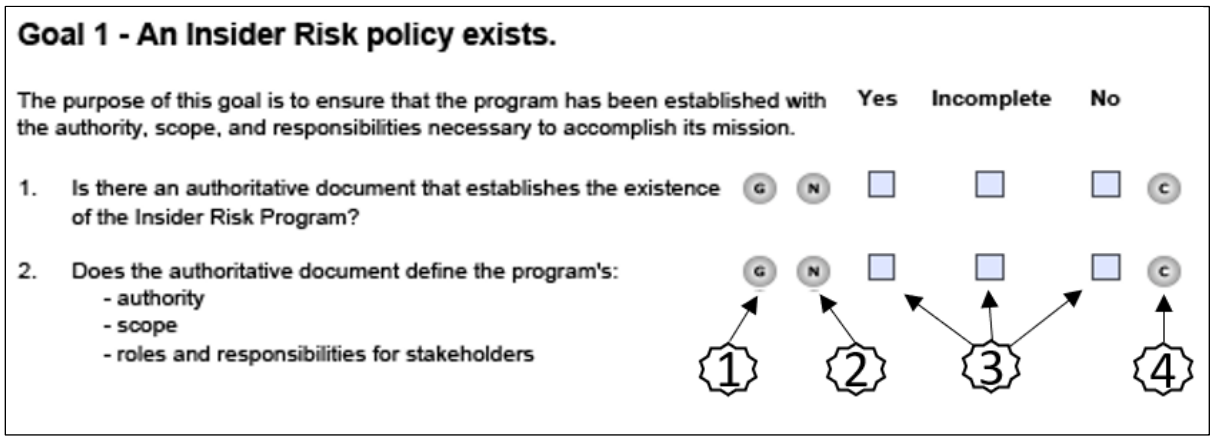

Figure 3: Answering Questions

When you answer a question in the tool, you can choose from the following options:

① Open question guidance.
② Open question notes.
③ Choose an answer.
④ Clear an answer.

2 Beginning a Self-Assessment

Typically, a *practitioner* and a *sponsor* use the IRMPE tool. A practitioner is a person who conducts the self-assessment. A sponsor is an overall leader of the assessment process. A sponsor should have a broad understanding of insider risk, and specific knowledge of the organization's insider risk program.

The practitioner has the following responsibilities:

- Delegates domain leads—one for each of the following IRMPE domains chosen during assessment scoping:
  - Program Management
  - Personnel and Training
  - Data Collection and Analysis
- Fills support roles as needed.
- Manages the completion of the assessment instrument for each domain.
- Generates IRMPE report(s).
- Distributes IRMPE report(s) to the sponsor and designees.
- Assists in the planning of follow-up activities.

The sponsor has the following responsibilities:

- Decides whether the organization should conduct an IRMPE.
- Selects the practitioner.
- Ensures that the resources necessary for the IRMPE are available.
- Communicates the organization's support for the IRMPE.

The sponsor and practitioner conduct the initial tasks of the IRMPE, then handoff to others in the organization who can support the assessment process and answer IRMPE questions. The *IRMPE User Guide* provides details on conducting an IRMPE within an organization, including an overview of the self-assessment process. (See Section 2 of the *IRMPE User Guide*.)

3 Processes of a Self-Assessment

This section is an overview of the process described in Section 3.1 of the *IRMPE User Guide*.

3.1 Self-Assessment Domains

An IRMPE includes three domains of assessment criteria:

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

An assessment can be scoped to any combination of these domains. The purpose of each domain is described below.

3.1.1 Program Management

The purpose of the Program Management domain is to determine whether an organization has the management structures, policies, relationships, and communications it needs as a foundation for an insider risk program. Program Management includes the following tasks:

- understanding mission critical assets
- defining the organization's insider risk policy
- characterizing the activities associated with insider threat prevention, detection, and response
- ensuring communication of insider threat activities and events among responsible participants in the organization's insider risk program
- providing governance and oversight of insider risk activities
- integrating insider risk management with organizational or enterprise risk management generally

3.1.2 Personnel and Training

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

- insider risk awareness training for all personnel
- role-based training for employees working with the insider risk team
- role-based training for insider risk program team members
- incorporation of insider risk training in the onboarding process

3.1.3 Data Collection and Analysis

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

organization's standards and policies and comply with relevant law and regulation. These key elements and process include the following:

- incident reporting
- forensics and behavioral analytics
- response mechanisms
- time-focused actions
- staff augmentation and organizational support
- other elements and procedures required to support an effective insider risk program
- Self-Assessment Domains

3.2 Identifying the Domain Leads and Courses of Action

The practitioner is responsible for identifying a lead for each domain selected to be part of the IRMPE scope. Each domain lead is responsible for identifying the subject matter experts (SMEs) who may need to be queried to answer questions in their assigned domain. Domain leads, in agreement and coordination with the practitioner, identify the courses of action (COA) for the IRMPE.

There are three primary COA:

3.2.1 COA1

For each domain, the domain lead answers the questions for the domain, consulting SMEs as needed. This COA may be preferred if the knowledge to answer the questions is largely available to the domain leads.

3.2.2 COA2

For each domain, the domain lead assembles a working group of SMEs to answer the domain questions. The domain lead leads the operation of this group and decides, for example, whether individual SMEs should answer subsets of the questions or whether the group should meet to collaboratively answer the domain questions. This COA may be preferred if the knowledge to answer the questions is distributed in the organization, and there is little overlap in the set of SMEs identified for the three domains.

3.2.3 COA3

The practitioner schedules one 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 in the organization, but there is significant overlap in the group of SMEs for the three domains leads.

General responsibilities of the domains leads include the following:

- identifying SMEs needed to answer questions for their domain
- meeting with SMEs to obtain answers to questions
- facilitating the completion of the assessment form in the instrument for their domain

3.3 Maturity Indicator Levels (MIL)

The practitioner selects a domain in the instrument, then reviews the set of goals for the domain. Each goal comprises a collection of questions. Goals are associated with capabilities at various maturity indicator levels (MILs):

MIL0 – Incomplete

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

MIL1 – Performed

This level 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

This level 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

This level 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

This level 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

This level indicates that all practices in an IRMPE domain are planned, managed, measured, and consistent across 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


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY