



CISA
CYBER+INFRASTRUCTURE



EXTERNAL DEPENDENCIES MANAGEMENT (EDM)

Assessment User's Guide

April 2020

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



Copyright 2019 Carnegie Mellon University.

The External Dependency Management (EDM) Assessment Package is based on the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both developed at Carnegie Mellon University's Software Engineering Institute. The government of the United States has at least a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, pursuant to the Rights in Technical Data-Noncommercial Items clauses (DFARS 252-227.7013 and DFARS 252-227.7013 Alternate I) contained in Federal Government Contract Number FA8702-15-D-0002.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

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.)

Internal Use: In addition to the Government's rights above, Carnegie Mellon University permits anyone to reproduce this material and to prepare derivative works from this material for internal use, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External Use: Additionally, 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. Permission can be requested at permission@sei.cmu.edu

®CERT is a registered trademark of Carnegie Mellon University.

DM19-0492

Table of Contents

1	Introduction	1
1.1	Purpose of This Guide	1
1.2	Intended Audience	1
1.3	How to Use This Guide	1
1.4	Organization of the Guide	2
2	EDM Assessment Overview	3
2.1	EDM Assessment Process	3
2.2	EDM Assessment Architecture	3
2.3	Domain Descriptions	5
	Relationship Formation (RF)	5
	Relationship Management and Governance (RMG)	5
	Service Protection and Sustainment (SPS)	5
2.4	MIL Scale	5
3	Conducting The EDM Assessment	9
3.1	Organizing for the Assessment	9
	Identifying the Scope of the Assessment	9
	Administering the EDM Assessment	10
	Key Roles in the Assessment Process	11
	Meeting with the Sponsor and Other Stakeholders	11
	Identifying and Preparing Participants	12
	Preparing for the Workshop	12
	During the Workshop	12
3.2	Completing the Assessment	14
	System Requirements and Setup	14
	Using the Assessment	14
	Generating the Report	17
4	Interpreting The EDM Assessment Report	18
4.1	EDM Assessment Scoring	18
	Basic Rules	18
	Scoring Rubric	18
4.2	How to Interpret the Report	19
	Scores	19
	NIST Cybersecurity Framework	23
	Options for Consideration	24
4.3	Identify Gaps	24
5	Making Improvements	26
5.1	Analyze Identified Gaps	27
	Setting a Target: Method 1	27
	Setting a Target: Method 2	27
5.2	Prioritize and Plan	28
5.3	Implement Plans	28



6 Summary	29
Appendix A: Process Checklist	30
Appendix B: EDM Assessment Glossary/Terms	33
Appendix C: References	37

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.

The 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.



List of Figures

Figure 1: The EDM Assessment Process	3
Figure 2: The External Dependency Management Assessment Domain Architecture	4
Figure 3: Profile Information	15
Figure 4: EDM Assessment Asset Categories	16
Figure 5: Explanatory Information	16
Figure 6: Entry Field for Other Observations	17
Figure 7: Buttons to Generate and Print the Report	17
Figure 8: EDM Assessment Performance Summary	20
Figure 9: Relationship Formation Individual Domain Report	21
Figure 10: EDM Assessment MIL-1 Performance Summary – Relationship Formation	22
Figure 11: EDM Assessment MIL-1 Performance – Relationship Formation	22
Figure 12: NIST Cybersecurity Framework Summary	23
Figure 13: Option for Consideration	24
Figure 14: Steps in a Typical Process Improvement Activity	25



List of Tables

Table 1: EDM Assessment Domain Composition	4
Table 2: Key Roles in the Assessment Process	11
Table 3: Identifying Participants	12
Table 4: Topics for Discussion at the Start of the Workshop	13
Table 6: Recommended Process for Using Results	26

1 INTRODUCTION

1.1 Purpose of This Guide

The purpose of this document is to enable organizations to conduct an assessment using the External Dependency Management Assessment (EDM Assessment) method. The EDM Assessment provides a measure of an organization's external dependency management capabilities. This user's guide

- presents an overview of the EDM Assessment structure and content
- provides information on how to prepare for an EDM Assessment
- provides information on how to conduct the assessment, which includes recording responses and scoring functions using the EDM Assessment tool
- assists the organization in evaluating its EDM management capabilities
- provides guidance for follow-on activities

The EDM Assessment 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 EDM Assessment to the NIST CSF is included as a component of the EDM Assessment Kit. Although the EDM Assessment can be used for this purpose, it is based on a different underlying framework¹ than the NIST CSF. As a result, an organization's fulfillment of EDM Assessment practices and capabilities may fall short of or exceed corresponding practices and capabilities in the NIST CSF.

The EDM Assessment reflects 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 EDM Assessment are designed to indicate the organization's ability to sustain EDM cybersecurity practices over time, the organization should not rely on the assessment results as a conclusive expression of the organization's cybersecurity capability in the future.

1.2 Intended Audience

This user's guide is intended for use by the individual who plans and facilitates an EDM Assessment. This individual is called the *facilitator*. The facilitator is typically accountable to a sponsor within the organization who has requested an EDM Assessment.

1.3 How to Use This Guide

The facilitator should use this guide as a starting point for preparing and executing the EDM Assessment. Sections 1 and 2 serve as an introduction to and overview of the EDM Assessment process. Sections 3 through 5 of the guide correspond to the three key phases of an assessment: EDM Assessment Form Completion, Report Interpretation, and Follow-Up. The facilitator should read through the entire guide and the supporting documents to become familiar with the EDM

¹ The EDM Assessment is based on the CERT® Resilience Management Model (CERT®-RMM).



Assessment itself as well as the end-to-end process of executing the assessment. Familiarity with the materials is important because each assessment is different and may require the facilitator to adapt the process and discussion to the needs of the organization being assessed. While the guide is intended to help ensure consistency of approach and data, there may be situations where some adjustments are necessary to ensure a valuable outcome for the organization being assessed.

1.4 Organization of the Guide

Section 2, EDM Assessment Overview, describes the EDM 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 an EDM Assessment, describes how the organization prepares for the assessment, conducts the assessment, and completes the form.
- Section 4: Interpreting the EDM 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 EDM management practices.

Section 6 provides a brief summary followed by the appendices, which contain a process checklist, a glossary of terms used in this document, and a list of references.

2 EDM ASSESSMENT OVERVIEW

2.1 EDM Assessment Process

The EDM Assessment is a lightweight assessment method that was created by the Department of Homeland Security (DHS) for the purpose of evaluating the external dependency management cybersecurity practices of critical infrastructure owners and operators. The EDM Assessment, consisting of 105 questions, is typically delivered in a four-hour session led by facilitators from DHS, or through a self-assessment process. The facilitators elicit answers from the critical infrastructure organization's personnel in cybersecurity, operations, physical security, and business continuity.

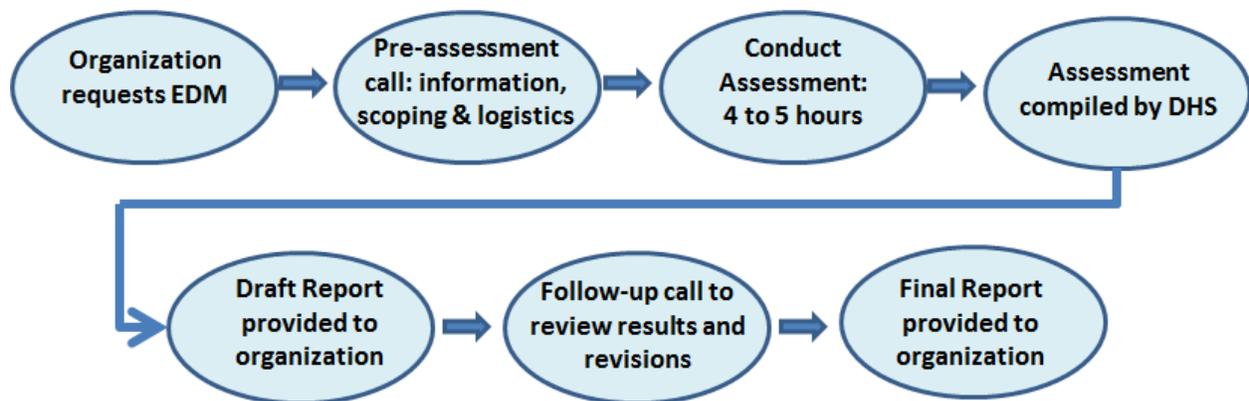


Figure 1: The EDM Assessment Process

2.2 EDM Assessment Architecture

The EDM Assessment is an interview-based assessment of an organization's cybersecurity management program, focused on the external dependencies of services and their associated assets which are critical for an organization's mission success. The EDM Assessment focuses on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization. The EDM Assessment measures essential external dependency cybersecurity capabilities and behaviors to provide meaningful indicators of an organization's operational resilience during normal operations and during times of operational stress.

The EDM Assessment is derived from the CERT[®] Resilience Management Model (CERT[®]-RMM), which was developed by the CERT Division at Carnegie Mellon University's Software Engineering Institute. The CERT-RMM is a capability-focused maturity model for process improvement, and it reflects best practices from industry and government for managing operational resilience across the disciplines of security management, business continuity management, and information technology operations management.

[®] CERT is a registered mark owned by Carnegie Mellon University.

Table 1 details the domains of the EDM Assessment. Each domain represents important capabilities that contribute to managing external dependencies across the lifecycle of the relationships with external organizations. The focus of EDM is on cybersecurity, in particular where information communications and technology (ICT) are involved in delivering essential services.

Table 1: EDM Assessment Domain Composition

EDM Assessment Domain	No. of Goals	No. of Goal Practices
Relationship Formation	6	26
Relationship Management and Governance	7	30
Service Protection and Sustainment	3	15
MIL Practices	4	15

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain. The EDM Assessment utilizes one standard set of Maturity Indicator Level (MIL) questions. The MIL questions examine the institutionalization of practices within an organization. Figure 2 graphically presents the EDM Assessment domain architecture. As shown in Table 1, the number of goals and practice questions varies by domain, but the set of MIL questions and the concepts they encompass are the same for all domains. All EDM Assessment questions have three possible responses: “Yes,” “No,” and “Incomplete.”

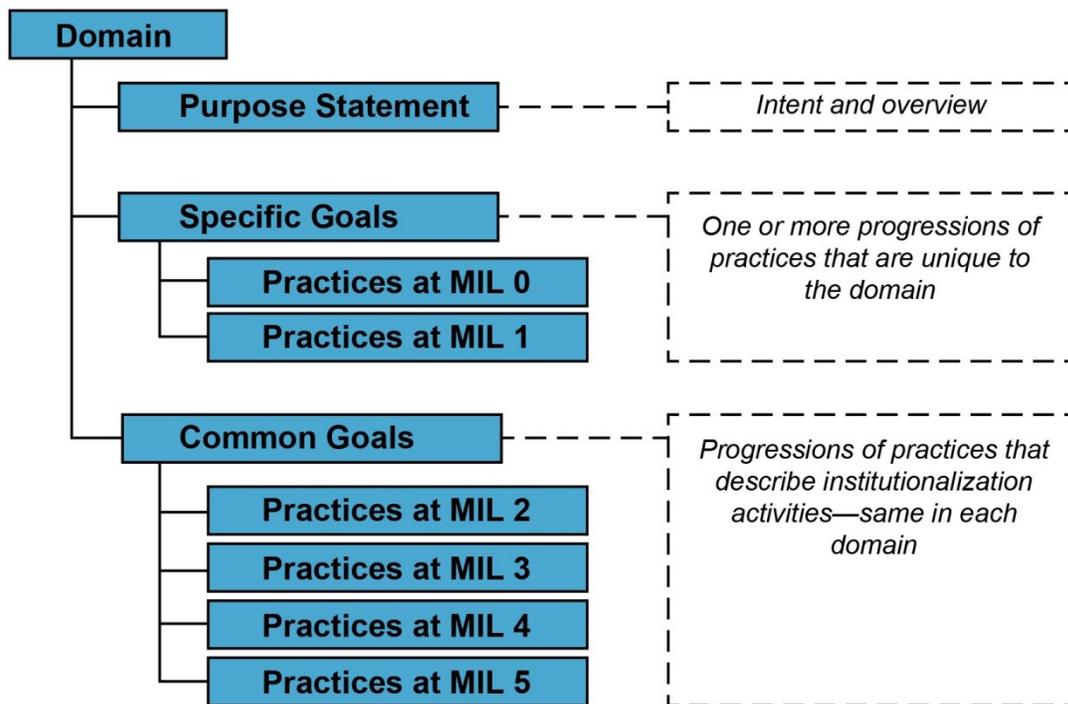


Figure 2: The External Dependency Management Assessment Domain Architecture



2.3 Domain Descriptions

The following section describes the three EDM Assessment domains and summarizes their goals and practice questions.

Relationship Formation (RF)

Domain comprises six goals and 26 practice questions:

Purpose: To assess whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them. Relationship Formation includes understanding the acquirer's critical services, having a process for entering into formal relationships, and evaluating external entities. A key aspect of Relationship Formation is identifying resilience requirements as the basis for risk management and formal agreements. Resilience requirements typically focus on integrity, confidentiality, and availability, but can also include other requirements important to the critical service.

Relationship Management and Governance (RMG)

Domain comprises seven goals and 30 practice questions:

Purpose: Relationship Management and Governance focuses on the extent to which the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk. This includes identifying the external entities that support the critical service, ongoing risk management, communicating with external entities about key aspects of protecting the critical service, and controlling external entities' access to the acquirer.

Service Protection and Sustainment (SPS)

Domain comprises three goals and 15 practice questions.

Purpose: The purpose of Service Protection and Sustainment is to assess whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats. This includes integrating external entity considerations into the acquirer's disruption planning—typically incident management and service continuity, validating controls at external entities, and maintaining situational awareness activities directed at external dependencies.

2.4 MIL Scale

The EDM Assessment uses Maturity Indicator Levels (MILs) to provide organizations with an approximation of the maturity of their practices in the three domains. The EDM Assessment's approach to maturity is based on an underlying capability maturity model, the CERT Resilience Management Model.² In this approach, the organization's maturity is based on how completely the cybersecurity practices in each of the domains are institutionalized within the organization.

² In its simplest form, a *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. The artifacts that make up

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 more 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 tighter alignment between cybersecurity activities and the organization’s business drivers. For example, in more mature organizations, managers will provide oversight to the particular domain and evaluate the effectiveness of the security activities the domain comprises.

The following example illustrates how MILs may be applied to the EDM Assessment Relationship Management and Governance domain in a fictitious organization:

Santa Barbara Manufacturing (SBM) is a medium-sized company that produces precision parts used in certain healthcare applications. The company benefits from having a skilled, capable Chief Information Security Officer (CISO). The CISO has worked hard to ensure that not only does SBM ensure quality control of its products to the highest safety standards, but that it also plans the processes around the availability and reliability of its critical vendors and suppliers. In other words, among other requirements, the company has a documented policy to govern the selection and supervision of its external partners and suppliers.

At the start of this fiscal year, a significant industry peer to SBM suffers a major incident because of a computer intrusion originating in another country. This incident causes SBM’s executive leadership to place additional emphasis on external dependency management. They begin to provide oversight to vendor management, ensure that staff and suppliers are qualified, and dedicate adequate funding to third-party management. They also evaluate and make decisions about the risks of deficiencies in the way that SBM and suppliers do contract management. This level of maturity is roughly equivalent to MIL3 Managed in the EDM Assessment.

As part of a strategic plan to diversify and grow the business, SBM is partnering with a company specializing in wireless medical equipment sales and payments management for healthcare providers. SBM plans to outsource its payments process to the smaller company, which brings new risks, such as those associated with suppliers who provide electronic processing of customer billing and payment information. To integrate external dependency management with the new business partner, SBM requires the partner assess its dependency management and achieve a MIL3 or better. To further support its dependency relationship, SBM develops procedures and processes that managers in the new company can use to adapt their management activities. The two business units also start to share lessons learned and improvements with each other. SBM is now starting to exhibit behavior characteristic of the EDM Assessment’s highest maturity level, MIL5 Defined.

the model are typically agreed to based on criteria fitting a particular domain or discipline, which are then validated through application and refinement.



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

Incomplete → Performed → Planned → Managed → Measured → Defined

These are described below:

MIL0 Incomplete

Practices in the domain are not being performed as measured by responses to the relevant EDM Assessment questions in the domain.

MIL1 Performed

All practices that support the goals in a domain are being performed as measured by responses to the relevant EDM Assessment questions.

MIL2 Planned

A specific practice in the EDM Assessment 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

All practices in a 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

All practices in a 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

All practices in a domain are performed, planned, managed, measured, and consistent across all constituencies within an organization who 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 only attain a given MIL if it has attained all lower MILs. In other words, an organization that fails to perform all of the cybersecurity practices at MIL1 in a domain would also fail to reach MIL2 in that domain, even if it would have satisfied all the requirements at MIL2.

The EDM Assessment uses one maturity scale for all three domains because the domains represent different parts of a lifecycle—from forming external relationships to managing incidents and consequences—rather than representing a fundamentally different capability. Ideally, senior management should manage, measure, and oversee the organization's external dependencies management capability across this complete lifecycle.

3 CONDUCTING THE EDM ASSESSMENT

3.1 Organizing for the Assessment

Identifying the Scope of the Assessment

Part of the facilitator's role is to help the sponsor and the organization identify the scope of the assessment. This scoping exercise is critical because answers to the assessment questions must be provided in relation to a specific service. The scope of the assessment is determined by three factors:

1. Critical service scope

Ask: Which service will be the focus of the assessment?

2. Organizational scope

Ask: Which parts of the organization deliver the critical service?

3. Asset scope

Ask: Which assets (people, technology, information, and facilities) are required for delivery of the service?

Critical Service Scoping

The EDM Assessment has a service-oriented approach, meaning that one of its foundational principles is that an organization and the external entities it utilizes deploy their assets (people, information, technology, and facilities) to support specific operational missions (or services).

The EDM Assessment uses the identified critical service to frame the questions in the assessment. Therefore it is essential that a critical service in your organization be identified that will serve as the focus of the assessment. A critical service is defined as follows:

A set of activities that the organization carries out, in the production of a product or while providing services to its customers, that are so important to the success of the organization that disruption to the service would severely impact the organization's operations or business.

The EDM Assessment strives to identify how an organization aligns its cybersecurity management activities and how it manages the external entities that may be involved with supporting the performance or production of the acquirer's critical services. Often, an organization's product suite provides a useful starting point for identifying a service. The following questions can help users identify their organization's critical services:

Which services compose a significant or intrinsic portion of the organization's mission (e.g., processing mortgage applications in a bank)?

Which services are externally focused (i.e., the service delivers value to stakeholders outside of the organization)?

Which services have identifiable ownership (i.e., authority) over assets that contribute to the delivery of the service?

Below are some examples of organizations and their typical critical services that might be selected as part of an EDM Assessment:

- banks and other financial institutions: clearing and settlement, mortgage application processing
- emergency services providers: processing 911 calls, dispatch
- electrical power plants: electricity generation, electricity distribution
- hospitals: clinical services, prescription management
- government agencies: court case management, benefit management
- manufacturing companies: machining operations, order processing
- airports: air traffic control, fuel management

Organizational Scoping

Organizational scoping considerations can be gathered by asking the following questions:

What part(s) of the organization is responsible for the delivery of the critical service?

Who are the owners of the assets required for delivery of the critical service?

Who is responsible for the critical service?

Who are the key stakeholders?

What asset types are used in the delivery of the service?

Who are key external entities that are used in the delivery of the service?

Who is the owner of the relationship(s) with supporting external entities?

What risks have been identified for the service?

Who are the custodians of the assets used in the delivery of the critical service?

Organizations may wish to consider including other units from within their organization as suppliers for the purposes of the assessment.

Administering the EDM Assessment

The EDM Assessment is conducted in a group setting with a facilitator leading a group discussion. During the course of the assessment, the facilitator guides participants to a group consensus for each answer. These participants, drawn from various departments (Line of business leaders, IT operations, Business Continuity, Risk Management, Vendor Management and others as appropriate), are subject matter experts (SMEs) who provide insight relevant to the different EDM

Assessment domains. The agreed-upon answer is then recorded in the assessment form before moving on to the next question.

This section describes planning for and conducting an assessment workshop. Sections 4 and 5 provide guidance for interpreting the resulting report and planning follow-on activities, respectively.

Key Roles in the Assessment Process

A successful EDM Assessment requires the active participation of members of the organization who serve in a variety of roles. Table 2 summarizes the key roles typically involved.

Table 2: Key Roles in the Assessment Process

Role	Description and Responsibilities
sponsor	The sponsor should have a broad understanding of the importance and components of the service for which the assessment is being completed. General responsibilities include <ul style="list-style-type: none"> • deciding whether the organization should conduct an EDM Assessment • selecting an individual to serve as the facilitator • ensuring that the resources necessary for the assessment are available • communicating the organization's support for the assessment
facilitator	The facilitator is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the EDM Assessment. General responsibilities include <ul style="list-style-type: none"> • completing the three phases of an assessment process • working with the organization to ensure the assessment produces high-quality results • facilitating the completion of the assessment form • generating the EDM Assessment report • distributing the EDM Assessment report to the sponsor and designees • assisting in the planning of follow-on activities
subject matter experts (SMEs)	During the assessment, SMEs provide answers that best represent the organization's current cybersecurity capabilities in relation to the function being evaluated. It is most helpful for a SME to be <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 setting a date for the planned assessment, the facilitator should meet with the sponsor and other stakeholders identified by the sponsor to prepare the organization for the assessment. The meeting should be scheduled a few weeks prior to the assessment.

The objectives of this meeting include the following:

- Familiarize the sponsor and/or stakeholders with the EDM Assessment.
- Obtain executive support and establish the role the sponsor wishes to play in the assessment.
- Shape the stakeholders' expectations for the assessment (e.g., the three phases of the process, required resources, timeframe involved, personnel roles and responsibilities).
- Answer any questions.

Identifying and Preparing Participants

For the EDM Assessment to be successful, participants should be knowledgeable about the organization's cybersecurity practices in relation to both the selected critical service and the external entities that are utilized to support the critical service identified. There should be SMEs familiar with how the organization operates in all three domains of the assessment (see Table 3). It is not necessary to have a single SME for each domain; one SME might cover multiple domains, or a single domain might require multiple SMEs.

Table 3: Identifying Participants

Domain/Expertise/Function	Name(s) of SME/Participant
Relationship Formation	
Relationship Management and Governance	
Service Protection and Sustainment	

In addition to SMEs discussed above, the facilitator should identify support staff whose assistance may be required during the assessment (e.g., scribes, IT support).

Preparing for the Workshop

Together with the sponsor and support staff, the facilitator schedules the workshop. An assessment typically takes two to four hours to complete. Assistance from the sponsor or executive management might be necessary to clear the calendars of SMEs and other critical participants.

Thorough logistical preparation is necessary to ensure a successful assessment workshop. In collaboration with support staff, the facilitator is expected to plan for all workshop logistics including reserving a room large enough to accommodate all participants and assuring that the necessary computing hardware and software are available (see Section 3.2 for system requirements).

During the Workshop

It is often useful to begin the workshop with comments from senior management. These comments can help emphasize the importance of the EDM Assessment to the organization, identify the business drivers for a cybersecurity effort, emphasize the importance of managing external entities, and highlight the importance of the active participation of workshop attendees.

The facilitator should remind participants that the survey is intended to provide a snapshot of the maturity of the organization's cybersecurity posture. Workshops like the EDM Assessment can provide a rare opportunity for discussion and teamwork across various departments, so it is worth reminding participants that they—not just the organization—can benefit from an honest and forthright discussion about the questions in the assessment. The facilitator should ensure that the workshop participants are prepared and comfortable during the workshop.

Table 4 describes several topics that previous EDM Assessments have shown to deserve special emphasis prior to beginning the workshop.

Table 4: Topics for Discussion at the Start of the Workshop

Topic	Discussion
Organization's vocabulary	This discussion covers terms found in the EDM Assessment that may prompt discussions relating to terms used within an organization.
Agreed-upon service and scope	It is important to remind the participants that the assessment is being applied to a specific critical service and only the set of activities performed by the organization and the external entities that support that critical service. It is useful to describe those activities and external relationships prior to beginning the workshop.
Organization's environment	It is useful to discuss the organization's environment to add context to the description of the service being evaluated.
Implemented practices	When completing the assessment, participants must consider practices as they are implemented on the day of the workshop. Do not consider activities that are planned or are in the process of implementation. Likewise, do not consider practices that have not been performed for extended periods of time. For example, if the organization has a disaster recovery plan that, in the opinion of the participants, is out of date to the point of being unusable, the plan should not be considered.
Three-point response scale	Participants use a three-point response scale to evaluate the degree to which the organization has implemented each practice. Review with the participants the meaning of each of the three response options so that all participants have a common understanding of when a particular response will be used.
Follow-on activities	It is important to discuss how the assessment will be used within the organization's overall cybersecurity program. Emphasize that next steps will be based on the organization's risks and maturity and point out the roles of participants in follow-on activities.

The facilitator guides the participants through the assessment questions. Remember that open dialog and consensus-building is as important as the completed assessment.

Most groups find it helpful to view a visual (projected) display of the survey. To begin, the facilitator shows participants the first questions from the Relationship Formation domain and reads the description of the domain, the first goal, and the first question verbatim. The facilitator 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 already provided. The facilitator controls the responses recorded on the assessment 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. There is value in allowing participants to interact and discuss as a group what the consensus answer will be. The facilitator 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 facilitator 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 times the facilitator must 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 is useful in coming to this understanding.

3.2 Completing the Assessment

The EDM Assessment Package is contained within a single Adobe PDF file titled *EDM Assessment v3*. The assessment provides the following:

- EDM Assessment question set with guidance
- collection method for answers
- automated scoring
- a report with the detailed results and suggested options for consideration

The PDF file comprises three sections: the cover material, the assessment form, and the report. Each section is discussed in detail below.

System Requirements and Setup

The package must be completed using Adobe Reader X or higher or Adobe Acrobat DC or higher on both the Windows and Mac operating systems. Using other, third-party PDF applications may result in erratic behavior and often results in corruption of the results. It may be necessary to enable Javascript within the PDF tool in order to complete the assessment.

Using the Assessment

The package enables simple collection of assessment data by using text fields, dropdown boxes, and checkboxes. It begins with basic profile information about the facilitator and organization (see Figure 3). The user will enter data by clicking in any field and typing the appropriate information. Pressing the Tab key or clicking in another field moves the user forward through the assessment.

Note this page includes a checkbox that represents a key scoping consideration: whether the assessment will include “other enterprise business units.” For some organizations, relationships with other parts of their organization are similar to relationships with external entities and can be treated as dependency risks by the assessment.

Organization Information

Facilitator

Name:

Title:

Phone: (enter numbers only, no spaces or other characters)

Email:

Date of EDM Assessment (Please use popup calendar):

Name of Organization:

Business Unit/Agency:

Organization Type (Industry, Federal Entity, [SLTI](#))

Sector:

Critical Service:

Please check this box if suppliers are scoped to include other enterprise business units:

Physical Location

City:

State:

Critical Service Point of Contact

Name:

Title:

Phone: (enter numbers only, no spaces or other characters)

Email:

Figure 3: Profile Information

The assessment portion of the form comprises checkboxes that provide preset answer options. Each question has three possible answers: “Yes,” “No,” and “Incomplete”:

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

The EDM Assessment divides assets into four categories: People, Information, Technology, and Facilities. Some questions require a separate answer for each of the four assets (see Figure 4) while other questions refer to all assets.

Goal 4 –Change and capacity management are applied to external dependencies.

The purpose of this goal is to assess whether the acquirer coordinates change and capacity management with external entities that support the critical service. A key part of this capability is the acquirer's own, internal change management process.

1. Does the acquirer have a **change management** process to manage modifications to its own assets that support the critical service? [ADM:SG3.SP2] 

	Yes	Incomplete	No
1.1 Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2 Technology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3 Facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.4 People	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 4: EDM Assessment Asset Categories

Each question has a *Clear* button  that can be used to clear out the answer to the question.

To aid the facilitator, each question is supported by guidance. Hovering over the  icon opens pop-up information that explains the question and answers (see Figure 5).

2. Do formal agreements require suppliers to manage their own external dependencies? [EXD:SP3.SP4, EXD:GG2.GP4]  

Question intent: To determine if the acquirer includes terms in formal agreements that require suppliers to manage their external dependencies.

Rarely do dependencies end with only the supplier with whom the acquirer is contracted. An external entity that fails to account for and manage its own external dependencies can represent an additional risk to the acquirer and critical service.

Typical work products

- Contract clauses that require suppliers to include similar requirements or clauses with their suppliers or sub-contractors

Criteria for “Yes” response

- The acquirer includes requirements in formal agreements with suppliers that the supplier will manage its own external dependencies to support the critical service.

Criteria for “Incomplete” response

- The acquirer includes requirements that some suppliers manage their own external dependencies, or the process to perform this practice is otherwise incomplete.

Additional guidance

Figure 5: Explanatory Information

At the end of each domain is a box labeled “Other Observations” (see Figure 6). Any text entered in this box is copied verbatim into the report. It can be used to capture information such as reasoning or organization-specific information. Facilitators should encourage notes to be taken as they allow for better recollection of issues/responses surrounding the assessment.

1 Relationship Formation

Relationship Formation – Other Observations

Figure 6: Entry Field for Other Observations

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

Generating the Report

Once the facilitator has entered all the information into the form and saved the file, a report is generated by clicking the *Generate Report* button located on the transition page (see Figure 7). A transition page is provided at both the beginning and the end of the assessment section for convenience. Adobe analyzes the answers and populates the report section of the document with results.

Once the report is generated, the report can be printed by clicking the *Print Report* button on the transition page. When viewing the report, note that the transition page is located immediately before the title page of the report.

PLEASE USE THE BUTTONS BELOW TO GENERATE THE REPORT,
REVISE THE ASSESSMENT, PRINT THE REPORT, OR PRINT THE
ASSESSMENT

Export Data Import Data Generate Report Print

Figure 7: Buttons to Generate and Print the Report

4 INTERPRETING THE EDM ASSESSMENT REPORT

4.1 EDM 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 MIL0 and MIL1 indicate base practice performance. Scores of MIL2 through MIL5 indicate institutionalization of practices.

Basic Rules

1. Practices are either performed (answer = “Yes”), incompletely performed (answer = “Incomplete”), or not performed (answer = “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” (grey)
- if “Not Answered” (grey) 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. CERT-RMM 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, which can be assigned only after a formal appraisal of capability maturity, not after using an assessment-based instrument.

4.2 How to Interpret the Report

Scores

The organization may use the EDM Assessment Report to create an action plan for addressing weaknesses and leveraging strengths identified in the assessment. A good place to start is with the EDM Assessment Performance Summary; Figure 8 shows an example.

It is important to note that a higher maturity level can only be achieved by an organization 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 MIL1 in a domain would also fail to reach MIL2 in that domain even if it satisfied (answered Yes to) all of the requirements at MIL2.

The MILs are an approximation of maturity in the organization. MILs describe attributes that would be *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 compare maturity across multiple domains. It is less useful as a rigorous, exact demonstration of a specific capability level in a single domain.

The performance summary may give some initial insights into where to invest in cybersecurity improvements by drawing attention to the absence of performed practices. As shown in Figure 8, the color-coded map of results by domain, combined with the individual domain results as shown in Figure 9, is useful for identifying areas for improvement.

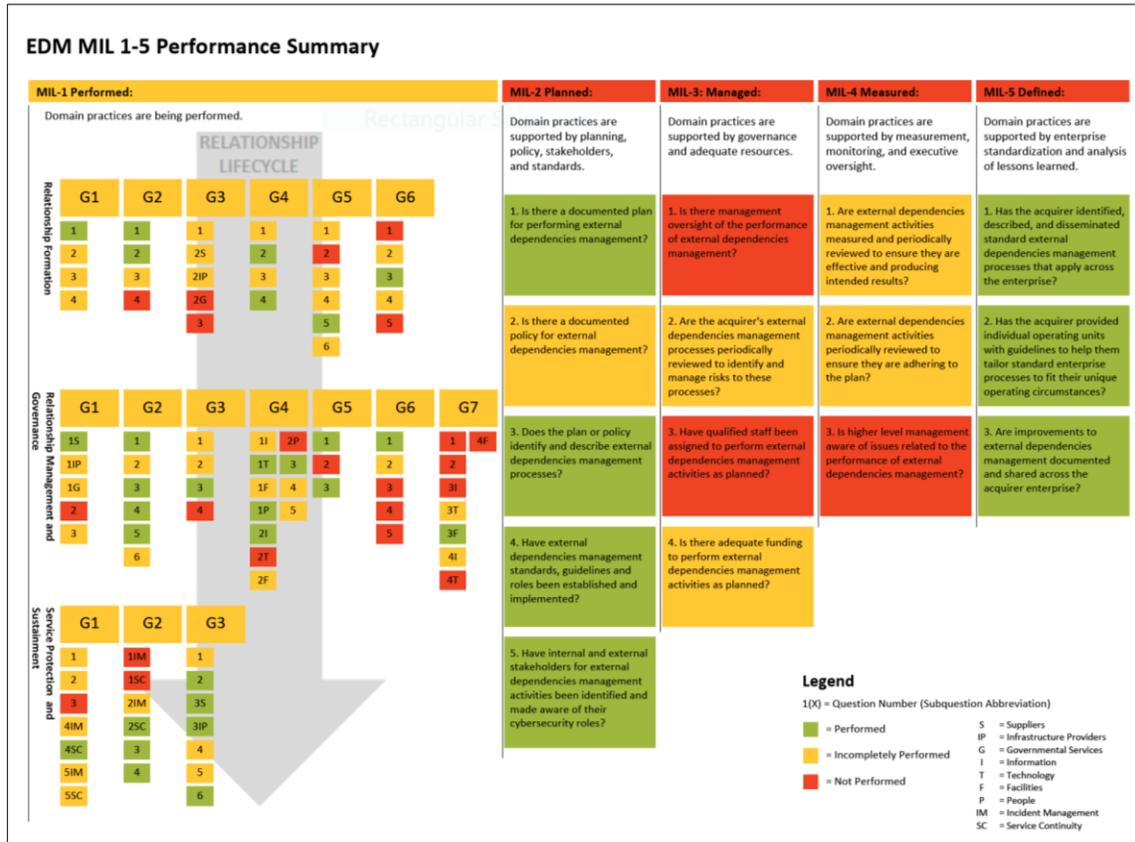


Figure 8: EDM Assessment Performance Summary

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 MIL1 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 relies on external vendors for the delivery of a critical service and no practices are being performed in the Relationship Formation domain, the organization may need to 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.

Individual domain reports, as shown in Figure 9, provide question-level detail to help organizations focus on specific practices for improvement.

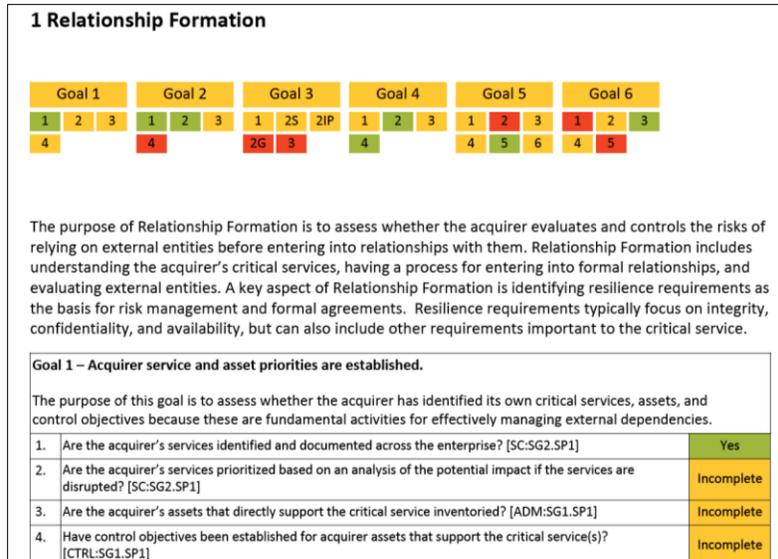


Figure 9: Relationship Formation Individual Domain Report

In the Relationship Formation scenario shown in Figure 9, the organization may benefit from focusing on the prioritization, review, and resilience requirements of the critical service in order to advance from the current MIL0 state to MIL1, as the organization is not yet performing all practices. The organization should focus on improvements in areas of highest risk rather than simply trying to achieve a higher MIL for its own sake.

The EDM Assessment MIL1 Performance Summary shown in Figure 10 provides an in-depth summary of MIL1 goals and practices for each EDM Assessment domain. The goal statement with a graphical depiction of the number of associated practices that are performed, incompletely performed, or not performed is provided. The summary of MIL1 practice performance is also provided for each domain and for the entire EDM Assessment.

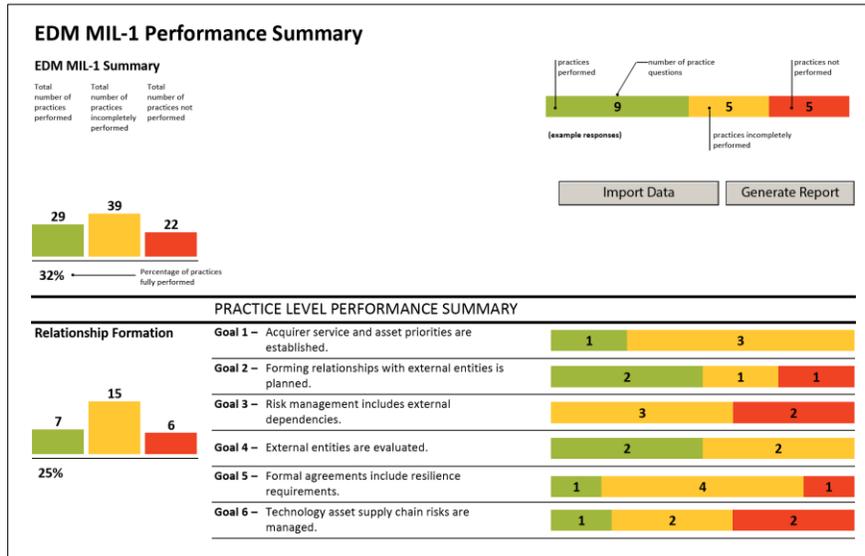


Figure 10: EDM Assessment MIL-1 Performance Summary – Relationship Formation

As with Figure 10, the EDM Assessment MIL1 Performance depiction shown in Figure 11 provides a fine level of operational detail. In the Relationship Formation scenario presented in Figure 11, the organization can determine that governmental services are not managed as well as other external dependency types. This view can be used to aid in identifying discrepancies in how dependencies are being managed.

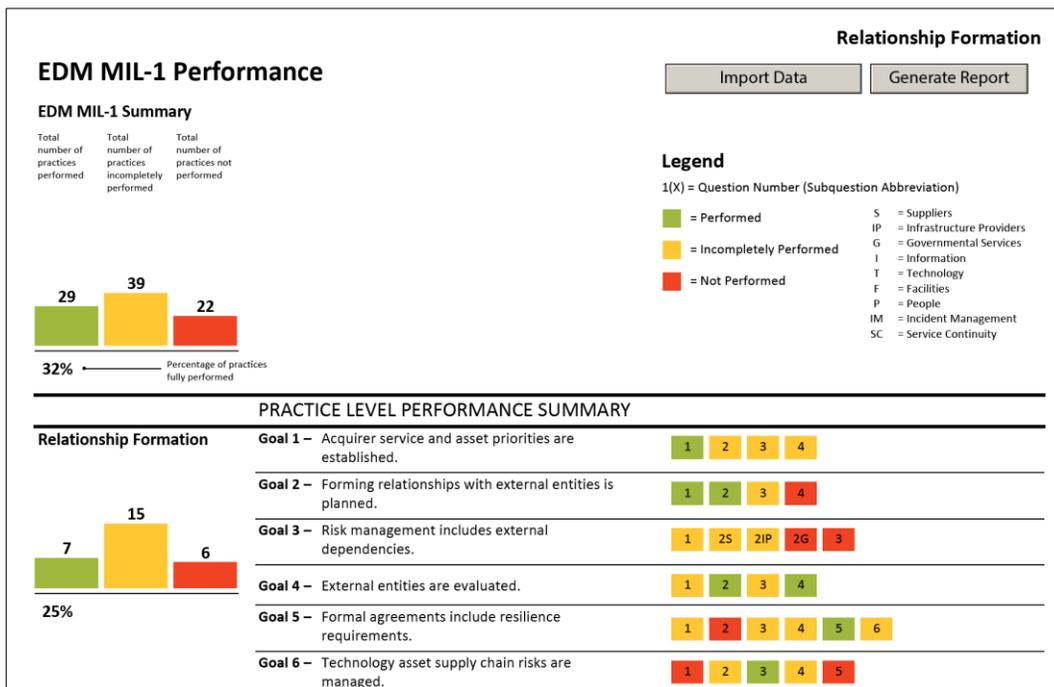


Figure 11: EDM Assessment MIL-1 Performance – Relationship Formation

NIST Cybersecurity Framework

The EDM Assessment also enables an organization to assess its capabilities relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Each EDM Assessment practice has been mapped to the applicable categories and subcategories of the NIST CSF. Figure 12 displays the organization's results by function and category. Bear in mind that there are sections of the CSF that do not map to the EDM because the assessment is focused on external dependencies and they will be clearly marked in the reports. An organization can use the summary of results to focus on prioritizing categories it chooses to improve. For example, while the organization is performing 33% of the practices that compose the Identify Function, the results also show that the organization is incompletely performing or not performing all the practices that relate to the Asset Management category. Therefore, the organization may choose to prioritize the implementation of practices that would lead to the improvement of the Asset Management category.

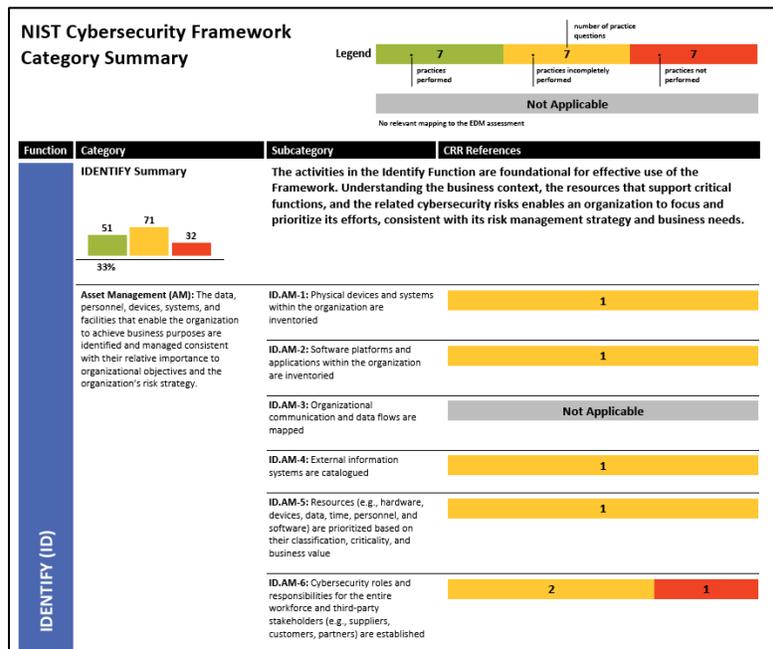


Figure 12: NIST Cybersecurity Framework Summary

Options for Consideration

The EDM Assessment Report includes a potential path toward improving the performance of each practice. These Options for Consideration are displayed in a grid below the organization's results for each goal in each domain (see Figure 13).

Q1	<p>CERT-RMM Reference [SC:SG2.SP1] Identify the acquirer's high-value services</p> <p>A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the acquirer's ability to achieve its mission. This practice refers to identifying the assessed acquirer's high-value services, which it provides to its customers and other stakeholders.</p> <p>Additional References <i>NIST Special Publication 800-53 Revision 4, "Recommended Security Controls for Federal Information Systems and Organizations" The Fundamentals, 2.1 Multitiered Risk Management.</i></p>
----	--

Figure 13: Option for Consideration

Options for Consideration are primarily sourced from the CERT-RMM and NIST special publications. Appendix C of this guide gives a full list of sources. The CERT-RMM options contain a root reference to the relevant specific goals and practices. This root reference has a standard pattern of abbreviation: *process area:specific goal.specific practice*. In Figure 13, the CERT-RMM reference for Question 1 (Q1) is to Service Continuity:Specific Goal 2.Specific Practice 1.

4.3 Identify Gaps

The EDM Assessment 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 infrastructure, resulting in a target maturity level for each domain
- review of provided Options for Consideration

Figure 14 demonstrates the iterative process of performing improvement activities.

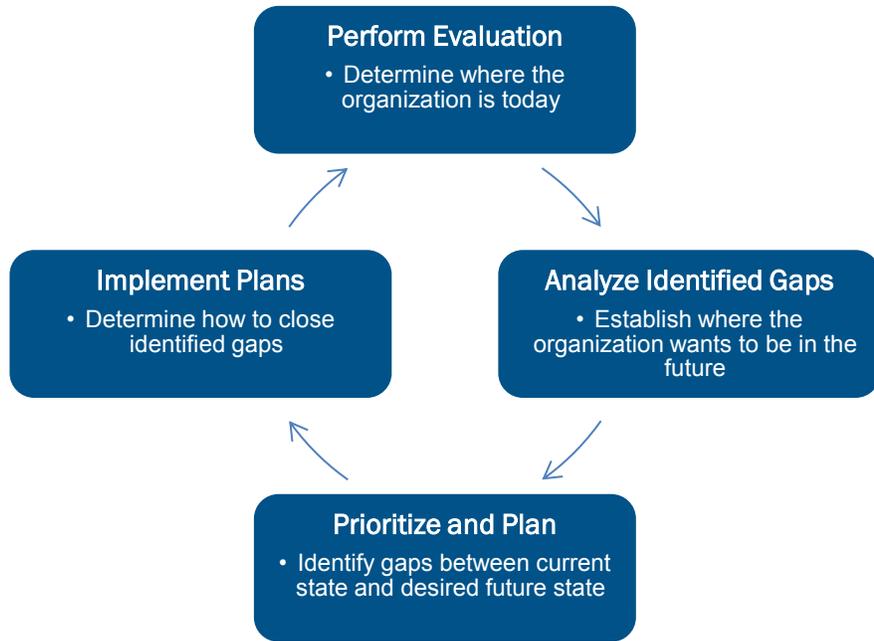


Figure 14: Steps in a Typical Process Improvement Activity

Table 5 demonstrates the initial workflow for the process improvement activities.

Table 5: EDM Assessment in the Process Improvement Workflow

	Inputs	Activities	Outputs
Perform Evaluation	1. EDM Assessment 2. Organizational policies and procedures 3. Understanding of current cybersecurity management and operations	1. Conduct the EDM Assessment	1. EDM Assessment Report

5 MAKING IMPROVEMENTS

The EDM Assessment does not prescribe the achievement of specific MILs for organizations in any particular sector. The EDM Assessment Report provides an organization with information on its current level of cybersecurity capabilities in each of the three EDM Assessment domains and can be used as a baseline for initiating a data-driven process improvement project, as depicted in Table 6.

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 6: Recommended Process for Using Results



	Inputs	Activities	Outputs
Analyze Identified Gaps	<ol style="list-style-type: none"> 1. EDM Assessment Report 2. Understanding the organization's objectives with respect to the critical service and its impact on critical infrastructure 	<ol style="list-style-type: none"> 1. Analyze gaps within the context of the organization (e.g., risk tolerance or threat profile) 2. Determine the potential impact of gaps to organizational objectives and impact on the critical service and on critical infrastructure 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, legislation) 	<ol style="list-style-type: none"> 1. Identify potential actions to address gaps 2. Perform cost-benefit analysis (CBA) for actions 3. Prioritize gaps and actions based on CBA 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 EDM Assessment Report provides graphs and tables that detail an analysis based on the recorded responses. Summary charts show achievement of MILs by domain, and detailed tables show the responses for each survey question. These graphs and tables show how the organization scores against the criteria of the EDM Assessment.

It is not 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 EDM Assessment to identify a desired target, is often adopted by organizations that are new to the EDM Assessment and have not previously established targets. The second approach, which involves walking through the practices before performing an Assessment, is most typically adopted by organizations that have more experience and familiarity with the EDM Assessment practices.

Setting a Target: Method 1

In this approach, an organization uses the results of a completed EDM Assessment to jump-start the identification of its target state. The organization begins by walking through its scores in each domain of the EDM 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 that practice.
4. If the practice does not need to be performed, then move on to the next practice for which there was 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 model domains.

Once 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 already performing, 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, an organization walks through the EDM Assessment 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 in the model and 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 model domains.

Once this review is complete, 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 can then be compared against 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 how gaps affect organizational objectives and critical 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 the actions needed.

Next, the organization should develop a plan to address the selected gaps. An organizational sponsor would ideally be the owner of the plan, though responsibility for implementation might 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 the risks to determine if changes to desired capability are needed. Periodic re-assessment using the EDM Assessment Package can track progress toward the organization's desired capability profile.



6 SUMMARY

This document describes the External Dependency Management Assessment (EDM Assessment) architecture and provides detailed descriptions of the three EDM Assessment domains and six Maturity Indicator Levels (MILs). This document also contains information about how to prepare for an EDM Assessment and how a facilitator assists the organization in assessing the maturity of its cybersecurity capabilities. It also gives guidance on follow-on activities to prioritize and implement a plan to close capability gaps that are identified through analysis of the EDM Assessment Report.

The EDM Assessment also provides an assessment of an organization's capabilities relative to the NIST Cybersecurity Framework (CSF). A reference crosswalk that maps the relationship of NIST CSF categories and subcategories to EDM Assessment goals and practices is included in the EDM Assessment Package.

For additional assistance, the facilitator and other participants can contact the Department of Homeland Security (DHS) at cse@hq.dhs.gov.

APPENDIX A: PROCESS CHECKLIST

EDM Assessment Checklist

Purpose: To guide the EDM Assessment process

Time	Item	Description	Completed
Four weeks prior to assessment workshop	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 workshop. 	<input type="checkbox"/>
Two weeks prior to assessment workshop	Facilities	Ensure that facilities have been set up correctly. <ul style="list-style-type: none"> • The room for the assessment workshop is large enough to hold all participants and any observers. • The room is set up to facilitate dialog among participants. • A projector and screen are available. • The lights in the room can be dimmed to ensure that projected information is readable. • One or more personal computers are available with Adobe Reader X or higher or Adobe Acrobat DC or higher. 	<input type="checkbox"/>
	Catering	Confirm catering, as applicable.	<input type="checkbox"/>



One week Availability Confirm that all participants are available and committed to attend the
prior to assessment workshop

Name	Title	Role (EDM Assessment Domain)
		RF
		RMG
		SPS

Sponsor Confirm that the sponsor is prepared to deliver opening remarks or has delegated this responsibility to another executive.

After the assessment workshop	Interpreting EDM Assessment Report	<p>Examine the EDM Assessment Report and answer the following questions: <input type="checkbox"/></p> <ul style="list-style-type: none"> • What are the overall strengths and weaknesses (see the Overall EDM Assessment Results chart in the report)? <ul style="list-style-type: none"> – What domains have not achieved at least MIL1? – 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 MIL1. – Identify the MIL practices that are not performed at MIL2 in the domains that have achieved MIL1.
--------------------------------------	------------------------------------	---

Analyzing gaps	Determine where the organization wants to be and what the gaps are. <input type="checkbox"/>	<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 future state, consider criteria such as the organization's business objectives and the criticality of the practice (or domain). • Compare the current state (the EDM Assessment Report) to the future 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 future state.
----------------	--	--

Prioritizing and planning	Prioritize the practices not currently performed that must be performed to achieve the future state. Consider criteria such as <input type="checkbox"/>	<ul style="list-style-type: none"> • how gaps affect organizational objectives and critical infrastructure • 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 <p>A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed.</p> <p>Create a plan to achieve the future state, using the prioritized list of identified practices that must be implemented.</p>
---------------------------	---	---

Implementing plan	Implement the plan. <input type="checkbox"/>	<ul style="list-style-type: none"> • Assign resources to implement the plan. • Periodically conduct assessments to measure progress. • Manage progress against the plan. • Re-plan as necessary.
-------------------	--	--

APPENDIX B: EDM ASSESSMENT GLOSSARY/TERMS

The following definitions are used in the EDM Assessment:

Acquirer – an organization that depends on external entities (vendors, infrastructure providers, public services, other business units in some cases) to fulfill its mission or business objectives. Acquirer refers to the assessed or subject organization, e.g., the organization undergoing the EDM Assessment

Assets – people, information, technology, and facilities that are used to provide the critical service being assessed. Several questions in the EDM Assessment refer to acquirer or external assets. These terms have the following meanings:

Acquirer assets – assets (people, information, technology, facilities) for which the acquirer is primarily responsible in terms of the assets' viability, productivity, and resilience

External assets – assets (people, information, technology, facilities) for which external entities are primarily responsible in terms of the assets' viability, productivity, and resilience

Capacity management – managing the demand for technology assets over a range of operational needs

Change management (change control) – a continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption

Control – a method, policy, or procedure—manual or automated—that is adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, administrative efficiency, and adherence to standards

Cooperative – describes activities or processes that are jointly performed by the acquirer and one or more external entities

Critical service – activities an organization carries out in the performance of a duty or in the production of a product that is essential to the organization's mission

Disruption management – activities to manage and mitigate the impact of events that may negatively affect the critical service. These usually involve activities such as incident management, problem management, service/ business continuity, or crisis planning.

Domain – in the context of the EDM Assessment, a domain is a logical grouping of external dependencies management practices that contribute to the cyber resilience of an organization.

Enterprise – the largest (i.e., highest level) organizational entity to which the acquirer belongs. For some participants, the acquirer is the enterprise itself.

External dependency – a condition in which the production and requirements of one or more products or services provided by the acquirer depend on the actions of an external entity. This is usually because the external entity is a supplier of goods or services to the acquirer; it has access to, ownership of, control of, responsibility for, or some other defined obligation relating to an asset that is important to the critical service.



Related terms:

Relationship: the existence of a connection, association or some level of external dependency

Formal agreement: a written agreement that creates obligations between the acquirer and an external entity. Formal agreements can provide clarity on terms, requirements, and responsibilities. Examples include contracts, service level agreements, or operational level agreements. Formal agreements are not required for an external dependency or relationship to exist.

External entity – an organization that is separate from the assessed acquirer or business unit. While these are frequently separate legal entities, they may also be separate business units, affiliates, or divisions within a large enterprise.

External entity types. The following are the definitions used in the EDM Assessment:

Supplier – an external entity that

1. supplies one or more of the following to the acquirer:
 - a. information and communications technology (ICT)
 - b. services supported by ICT
 - c. services that support the acquirer's operation or sustainment of ICT, and
2. with which the acquirer has some ability to negotiate the terms and conditions of agreements that govern the acquirer-supplier relationship

Suppliers may also be known subcontractors, vendors, or separate divisions or affiliates of a large enterprise.

Governmental services – a service provided to people, organizations, or other entities in a political subdivision (nation, state, or locality), usually provided by a governmental department or agency. These services frequently involve security: for example fire, police, and emergency response. Non-emergency examples include the U.S. Postal Service and transportation management and support agencies (federal and state agencies, regional port authorities, etc.).

Industry consortia – voluntary groups of private industry or public stakeholders working cooperatively to minimize cybersecurity and external dependency risk. This activity frequently involves exchanging information about risks and threats.

Infrastructure providers – a type of supplier that supplies goods or services to a region, economy, infrastructure sector, or political subdivision, and with which the acquirer normally has no commercially practical ability to negotiate the terms and conditions of agreements. Contracts with infrastructure providers are generally “take it or leave it.”¹ Examples include natural gas, water, power, or transportation.

Trusted supplier (ICT) – a supplier that provides information and communications technology to the acquirer, which the acquirer has justifiable reason to believe meets appropriate standards for the use intended. One way for the supplier to achieve this is by demonstrating compliance with standards set forth by an acknowledged authority to ensure the integrity of the technology purchased. The authority may be the original equipment manufacturer or an appropriate industry body (such as The Open Group, International Standards Organization, or similar body). Well-established experience with suppliers may also establish trust. NIST Special Publication 800-53 states “services provided to organizations through well-established . . . business relationships may provide degrees of trust in such services within the tolerable risk range of the authorizing officials and organizations using the services.”



Using a trusted ICT supplier cannot provide complete protection against vulnerabilities, malicious tampering, or counterfeit ICT; however, it does indicate the presence of management controls against this specific risk.

High value service – see critical service

ICT Supply Chain – linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.²

Incident – an event (or series of events) that significantly affects (or has the potential to significantly affect) assets and services and requires the acquirer (and possibly external entities) to respond in some way to prevent or limit adverse impacts.

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.

Operational resilience – the organization's ability to adapt to risk that affects its core operational capabilities. Operational resilience is the emergent property of an organization to continue to survive and carry out its mission after disruption that does not exceed its operational limit.

Operational risk – potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence. Managing risk in the EDM Assessment focuses on operational risks involving the actions of people, technology failures, failed internal processes, and disruptive external events. Operational risk is distinct from, but related to, other enterprise risk areas such as financial and market risk.

Plan – a detailed, written formulation of a program of action to satisfy or perform a practice or goal in the EDM Assessment. At higher maturity levels (MIL2 - Planned) the plan is a document to support the acquirer's performance of External Dependencies Management as an organizational capability.

Policy – a high-level, overall plan embracing the general goals and acceptable procedures of an organization

Practice – an activity performed to support a domain goal

Process – a series of actions or steps taken in order to achieve a particular EDM practice or goal

¹ The key difference between a supplier and an infrastructure provider, from the perspective of External Dependencies Management, is that acquirers normally have a very limited ability to negotiate the terms of the relationship with infrastructure providers. Note that this is a relative standard. In other words, large acquirers that *do* have the ability to negotiate terms with infrastructure providers may wish to treat these external entities as suppliers for the purpose of an Assessment. Because the EDM Assessment is intended for critical infrastructure organizations of different sizes, this is intended to be a flexible definition.

² *National Institute of Standards and Technology, NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, October 2012, p. 75.*



Resilience requirement – a constraint that the acquirer places on internal or external assets to ensure they remain viable and sustainable when charged into production to support a service. These are often expressed in terms of confidentiality, integrity, or availability. Resilience requirements help ensure the protection of high-value assets as well as their continuity when an incident or disruption occurs.

Risk – see Operational risk.

Service – a set of activities the acquirer carries out in the performance of a duty or in the production of a product

Situational awareness – the purpose of situational awareness is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise.

Stakeholder – a person or organization that has a vested interest in the organization or its activities

Threat – the combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the acquirer

Vulnerability – a characteristic of design, location, security posture, operation, or any combination thereof that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation

APPENDIX C: REFERENCES

*A Complete Guide to the Common Vulnerability Scoring System Version 2.0
Security Incident Response Teams (CSIRTs)*

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305>

NIST Cybersecurity Framework

<https://www.nist.gov/cyberframework>

Managing for Enterprise Security

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7019>

Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems

<https://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>

Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments

https://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Special Publication 800-34, Contingency Planning for Federal Information Systems

https://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Special Publication 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems

<https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>

Special Publication 800-39, Managing Information Security Risk Organization, Mission, and Information System View

<https://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>

Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

Special Publication 800-53 Revision 5 (Draft), Security and Privacy Controls for Information Systems and Organizations

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft>

Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>



Special Publication 800-70 Revision 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf>

Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf>

Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems

<https://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf>

Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

<https://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>



Homeland
Security