CYBER RESILIENCE REVIEW (CRR)

Assessment User Guide

Adapted for CSET® December 2021. Original publication April 2020.

Table of Contents

1 Introduction 6
1.1 Purpose of This Guide 6
Intended Audience 6
How to Use This Guide 6
1.2 Organization of the Guide 7
2 CRR Overview 8
CRR Method 8
2.1 CRR Architecture 10
2.2 Domain Descriptions 11
Asset Management (AM) 13
Controls Management (CM) 15
Configuration and Change Management (CCM) 16
Vulnerability Management (VM) 17
Incident Management (IM) 18
Service Continuity Management (SCM) 20
Risk Management (RM) 21
External Dependencies Management (EDM) 22
Training and Awareness (TA) 23
Situational Awareness (SA) 24
2.3 MIL Scale 25
3 Conducting A CRR Assessment 28
Organizing for the Assessment 28
Identifying the Scope of the Assessment 28
Administering the CRR Assessment 29
Key Roles in the Assessment Process 29
Meeting with the Sponsor and Other Stakeholders 30
Identifying and Preparing Participants 30
Preparing for the Workshop 31
During the Workshop 31
3.1 Getting Started with the CRR Assessment in CSET® 34
System Requirements and Setup 34
3.2 Tutorial: Using the CSET® CRR Assessment Software 39
Practice Question Structure 39
4 CRR Assessment Results and Report 43
4.1 CRR Scoring 45
Basic Rules 45
Scoring Rubric 45
4.2 How to Interpret the Report 46
Scores 46
NIST Cybersecurity Framework Scoring Depictions 53
Options for Consideration 57
4.3 Identify Gaps 58
5 Making Improvements 60
5.1 Analyze Identified Gaps 61
Setting a Target: Method 1 61

Setting a Target: Method 2 61
Prioritize and Plan 63
Implement Plans 64
6 Summary 65
Appendix A: Process Checklist 66
Appendix B: CRR Glossary/Terms 69
Appendix C: References 75

List of Figures

Figure 1: The Cyber Resilience Review Domain Architecture 11
Figures 2-2.3: Getting Started with the CRR Assessment in CSET 34
Figure 3: Assessment Question Structure 39
Figure 4: Domain Remarks Field 41
Figure 5: Asset Types 42
Figure 6: Reports Function 43
Figure 7: CRR Report Menu with Download Report (PDF) Function 44
Figure 8: CRR Performance Summary 47
Figure 9: A Sampling of Individual Domains 48
Figure 10:Asset Management Individual Domain Report 48
Figure 11:Controls Management Individual Domain Report 49
Figure 12: CRR MIL-1 Performance Summary – Asset Management 50
Figure 13:CRR MIL-1 Performance – Vulnerability Management 50
Figure 14: CRR Performance View 51
Figure 15: Summary of CRR Results 52
Figure 16: Percentage of Practices Completed by Domain 53
Figure 17: NIST Cybersecurity Framework Summary 54
Figure 18: NIST Cybersecurity Framework Category Summary 55
Figure 19: NIST Cybersecurity Framework Category Performance 56
Figure 20: Options for Consideration 57
Figure 21: Steps in a Typical Process Improvement Activity 60

List of Tables

Table 1: CRR Domain Composition 4
Table 2: Key Roles in the Assessment Process 20
Table 3: Identifying Participants 21
Table 4: Topics for Discussion at the Start of the Workshop 22
Table 5: Recommended Process for Using Results 39

1 INTRODUCTION

1.1 Purpose of This Guide

The purpose of this document is to enable organizations to conduct an assessment using the Cyber Resilience Review (CRR). The CRR Assessment provides a measure of an organization's cyber resilience capabilities. This user guide:

- presents an overview of the CRR structure and content
- provides information on how to prepare for an assessment
- provides information on how to conduct the assessment, which includes recording responses and scoring functions
- assists the organization in evaluating its cyber resilience capabilities
- provides guidance for follow-on activities.

The CRR Assessment also enables an organization to assess its capabilities relative to v1.1 of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and a crosswalk document that maps the CRR to the NIST CSF is included as a component of the CRR Assessment Kit. Though the CRR can be used for this purpose, it is based on a different underlying framework[1] than the NIST CSF. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of or exceed corresponding practices and capabilities in the NIST CSF.

The CRR reflects an organization's capabilities only at the time of the assessment. Even though certain aspects and questions in the CRR are designed to indicate the organization's ability to sustain 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.

Intended Audience

This user's guide is intended for use by the individual selected by the organization to plan and facilitate a CRR Assessment. This individual is called the *facilitator*. The facilitator is typically accountable to a sponsor within the organization who has requested a CRR Assessment.

How to Use This Guide

The facilitator should use this guide as a starting point for preparing and executing the CRR Assessment. Sections 3 through 5 of the guide correspond to the three key phases of an assessment: CRR Assessment Completion, Report Interpretation, and Follow- Up. The facilitator should read through the entire guide and the supporting documents to become familiar with the CRR 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 move through this guide not in the order the material is presented. There also may be some iteration of activities.

1.2 Organization of the Guide

Section 2
The CRR Overview section describes the CRR architecture as well as the individual components that make up the CRR.

Sections 3 through 5
The three key phases of a typical assessment process are described:

- **Section 3:** Conducting a CRR Assessment. The organization prepares for the assessment, conducts the assessment, and completes the assessment.

- **Section 4:** Interpreting the CRR Assessment Report. The results documented in the assessment report are interpreted within the context of the organization.

- **Section 5:** Making Improvements. The organization determines next steps for improving its cybersecurity practices.

Section 6
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 CRR OVERVIEW

CRR Method

The CRR is a lightweight assessment method that was created by the Cybersecurity and Infrastructure Security Agency (CISA) for the purpose of evaluating the cybersecurity and service continuity practices of critical infrastructure owners and operators. The CRR, consisting of 299 questions, is typically delivered in a six-hour workshop led by facilitators from CISA. The facilitators elicit answers from the critical infrastructure organization's personnel in cybersecurity, operations, physical security, and business continuity.

The CRR Assessment Package allows organizations to apply the same method without the participation of external facilitators. It contains the same questions, scoring mechanisms, and options for improvement as the externally facilitated CRR.

2.1 CRR Architecture

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

The CRR 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.

Table 1 details the domains of practice that the CRR examines. Each domain represents important capabilities that contribute to the cyber resilience of an organization.

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

Table 1: CRR Domain Composition

CRR Domain	No. of Goals	No. of Goal Practices	No. of MIL* Practices
Asset Management	7	30	13
Controls Management	4	16	13
Configuration and Change Management	3	23	13
Vulnerability Management	4	15	13
Incident Management	5	23	13
Service Continuity Management	4	16	13
Risk Management	5	13	13
External Dependencies Management	5	14	13
Training and Awareness	2	11	13
Situational Awareness	3	8	13

* Maturity Indicator Level

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of Maturity Indicator Level (MIL) questions. The MIL questions examine the institutionalization of practices within an organization. Figure 1 graphically presents the CRR 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 CRR questions have three possible responses: “Yes,” “No,” and “Incomplete.”

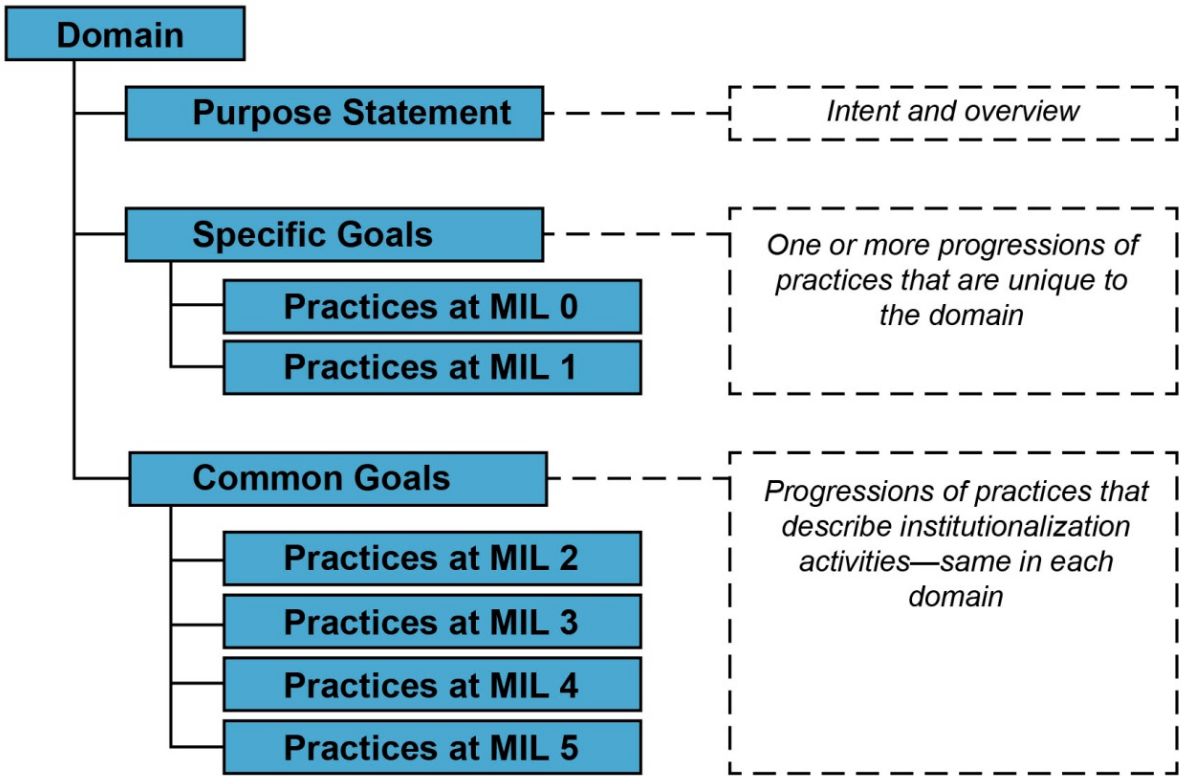

Figure 1: The Cyber Resilience Review Domain Architecture

2.2 Domain Descriptions

The following section describes the 10 CRR domains and summarizes their goals and practices.

Asset Management (AM)

Purpose: To identify, document, and manage assets during their lifecycle to ensure sustained productivity to support critical services.

The Asset Management domain establishes a method for an organization to plan, identify, document, and manage its assets. Assets are the raw materials that services need to operate. The CRR organizes assets into the following categories:

- *People* to operate and monitor the service
- *Information* and data to feed the process and to be produced by the service
- *Technology* to automate and support the service
- *Facilities* in which to perform services

The Asset Management domain comprises seven goals and 30 practices:

1. Services are identified and prioritized.
• The organization's services are identified.
• The organization's services are prioritized based on analysis of the potential impact if the services are disrupted.
• The organization's mission, vision, values, and purpose, including the organizations place in critical infrastructure, is identified and communicated.
• The organization's mission, objectives, and activities are prioritized.

2. Assets are inventoried, and the authority and responsibility for these assets is established.
• The assets that directly support the critical service are inventoried (technology includes hardware, software, and external information systems).
• Asset descriptions include protection and sustainment requirements.
• Owners and custodians of assets are documented in asset descriptions.
• The physical locations of assets (both within and outside the organization) are documented in the asset inventory.
• Organizational communications and data flows are mapped and documented in the asset inventory.

3. The relationship between assets and the services they support is established.
• The associations between assets and the critical service they support are documented.
• Confidentiality, integrity, and availability requirements are established for each service-related asset.

4. The asset inventory is managed.
• Change criteria are established for asset descriptions.
• Asset descriptions are updated when changes to assets occur.

5. Access to assets is managed.
• Access (including identities and credentials) to assets is granted based on their protection requirements.

• Access (including identities and credentials) requests are reviewed and approved by the asset owner.
• Access privileges are reviewed to identify excessive or inappropriate privileges.
• Access privileges are modified as a result of reviews.
• Access permissions are managed incorporating the principle of least privilege.
• Access permissions are managed incorporating the principle of separation of duties.
• Identities (e.g., user accounts) are proofed before they are bound to credentials that are asserted in interactions.

6. Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
• Information assets are categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, or secret).
• The categorization of information assets is monitored and enforced.
• Policies and procedures for the proper labeling and handling of information assets are created.
• All staff members who handle information assets (including those who are external to the organization, such as contractors) are trained in the use of information categories.
• High-value information assets are backed up and retained.
• Guidelines for properly disposing of information assets are created.
• Adherence to information asset disposal guidelines is monitored and enforced.

7. Facility assets supporting the critical service are prioritized and managed.
• Facilities are prioritized based on their potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities.
• The prioritization of facilities is reviewed and validated.
• Protection and sustainment requirements of the critical service are considered during the selection of facilities.

Controls Management (CM)

Purpose: To identify, analyze, and manage controls in a critical service's operating environment.

Internal control is a governance process used by an organization to ensure effective and efficient achievement of organizational objectives and to provide reasonable assurance of success. The Controls Management domain outlined in the CRR presents a way for the organization to identify control objectives and establish controls to meet those objectives. The Controls Management domain also addresses the importance of analyzing and assessing those controls to ensure that the process is constantly being improved.

The Controls Management domain comprises four goals and 16 practices:

1. Control objectives are established.
• Control objectives are established for assets required for delivery of the critical service.
• Control objectives are prioritized according to their potential to affect the critical service.

2. Controls are implemented.
• Controls are implemented to achieve the control objectives established for the critical service.
• Controls are implemented, incorporating network segregation where appropriate, to protect network integrity.
• Controls are implemented to protect data at rest.
• Controls are implemented to protect data in transit.
• Controls are implemented to protect against data leaks.
• Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
• Controls are implemented to protect and restrict the use of removable media in accordance with policy.
• Controls are implemented to protect communication and control networks.
• Cybersecurity human resource practices are implemented for the critical service (e.g., de-provisioning, personnel screening).
• Access to systems and assets is controlled by incorporating the principle of least functionality (e.g., allowlisting, blocklisting, etc.).

3. Control designs are analyzed to ensure they satisfy control objectives.
• Control designs are analyzed to identify gaps where control objectives are not adequately satisfied.
• As a result of the controls analysis, new controls are introduced, or existing controls are modified to address gaps.

4. The internal control system is assessed to ensure control objectives are met.
• The performance of controls is assessed on a schedule to verify they continue to meet control objectives.
• As a result of scheduled assessments, new controls are introduced or existing controls are modified to address problem areas.

Configuration and Change Management (CCM)

Purpose: To establish processes to ensure the integrity of assets, using change control and change control audits.

An organization's asset infrastructure is constantly evolving as technology changes, information is updated, and new personnel are hired. The Configuration and Change Management domain addresses how an organization can implement processes and procedures that manage assets and ensure that changes made to those assets are minimally disruptive to the organization.

The Configuration and Change Management domain comprises three goals and 23 practices:

1. The lifecycle of assets is managed.

• A change management process is used to manage modifications to assets.
• Resilience requirements are evaluated as a result of changes to assets.
• Capacity management and planning are performed for assets.
• Change requests are tracked to closure.
• Stakeholders are notified when they are affected by changes to assets.
• A System Development Life Cycle is implemented to manage systems supporting the critical service.

2. The integrity of technology and information assets is managed.

• Configuration management is performed for technology assets.
• Techniques are used to detect changes to technology assets.
• Modifications to technology assets are reviewed.
• Integrity requirements are used to determine which staff members are authorized to modify information assets.
• The integrity of information assets is monitored.
• Unauthorized or unexplained modifications to technology assets are addressed.
• Modifications to technology assets are tested before being committed to production systems.
• A process for managing access to technology assets is implemented.
• The maintenance and repair of assets is performed and logged in a timely manner.
• The maintenance and repair of assets is performed with approved and controlled tools and/or methods.
• The remote maintenance and repair of assets is approved, logged, and performed in a manner that prevents unauthorized access.

3. Asset configuration baselines are established.

• Technology assets configuration baselines are created.
• Approval is obtained for proposed changes to baselines.
• A baseline of network operations is established.
• The baseline of network operations is managed.
• A baseline of expected data flows for users and systems is established.
• The baseline of expected data flows for users and systems is managed.

Vulnerability Management (VM)

Purpose: To identify, analyze, and manage vulnerabilities in a critical service's operating environment.

Vulnerability is the susceptibility of an asset, and the associated critical service, to disruption. Vulnerabilities can result in operational risks and must be identified and managed to avoid disruptions to the critical service's operating environment. A vulnerability management process identifies and analyzes vulnerabilities before they are exploited and informs the organization of threats that must be analyzed in the risk management process to determine whether they pose tangible risk to the organization based on the organization's risk tolerance.

The Vulnerability Management domain comprises four goals and 15 practices:

1. Preparation for vulnerability analysis and resolution activities is conducted.
• A vulnerability analysis and resolution strategy has been developed.
• There is a standard set of tools and/or methods in use to identify vulnerabilities in assets.
• A standard set of tools and/or methods is in use to detect malicious code in assets.
• A standard set of tools and/or methods is in use to detect unauthorized mobile code in assets.
• A standard set of tools and/or methods is in use to monitor assets for unauthorized personnel, connections, devices, and software.

2. A process for identifying and analyzing vulnerabilities is established and maintained.
• Sources of vulnerability information have been identified.
• The information from these sources is kept current.
• Vulnerabilities are being actively discovered.
• Vulnerabilities are categorized and prioritized.
• Vulnerabilities are analyzed to determine relevance to the organization.
• A repository is used for recording information about vulnerabilities and their resolution.

3. Exposure to identified vulnerabilities is managed.
• Actions are taken to manage exposure to identified vulnerabilities.
• The effectiveness of vulnerability mitigation is reviewed.
• The status of unresolved vulnerabilities is monitored.

4. The root causes of vulnerabilities are addressed.
• Underlying causes for vulnerabilities are identified (through root-cause analysis or other means) and addressed.

Incident Management (IM)

Purpose: To establish processes to identify and analyze events, detect incidents, and determine an organizational response.

Disruptions to an organization's operating environment regularly occur. The Incident Management domain examines an organization's capability to recognize potential disruptions, analyze them, and determine how and when to respond.

The Incident Management domain comprises five goals and 23 practices:

1. A process for identifying, analyzing, responding to, and learning from incidents is established.
• The organization has a plan for managing incidents.
• The incident management plan is reviewed and updated.
• The roles and responsibilities in the plan are included in job descriptions.
• Staff has been assigned to the roles and responsibilities detailed in the incident management plan.

2. A process for detecting, reporting, triaging, and analyzing events is established.
• Events are detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information).
• Event data is logged in an incident knowledgebase or similar mechanism.
• Events are categorized.
• Events are analyzed to determine if they are related to other events.
• Events are prioritized.
• The status of events is tracked.
• Events are managed to resolution.
• Requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes are identified.
• A process to ensure event evidence is handled as required by law or other obligations is followed.

3. Incidents are declared.
• Incidents are declared.
• Criteria for the declaration of an incident are established.
• Incidents are analyzed to determine a response.

4. A process for responding to and recovering from incidents is established.
• Incidents are escalated to stakeholders for input and resolution.
• Responses to declared incidents are developed and implemented according to pre- defined procedures.
• Incident status and response is communicated to affected parties (including public relations staff and external media outlets).
• Incidents are tracked to resolution.

5. Post-incident lessons learned are translated into improvement strategies.
• Analysis is performed to determine the root causes of incidents.

• A link between the incident management process and other related processes (problem management, risk management, change management, etc.) is established.
• Lessons learned from incident management are used to improve asset protection and service continuity strategies.

Service Continuity Management (SCM)

Purpose: To ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other event.

The process of assessing, prioritizing, planning, and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of the critical services.

The Service Continuity Management domain comprises four goals and 16 practices:

1. Service continuity plans for high-value services are developed.
• Service continuity plans are developed and documented for assets (people, information, technology, and facilities) required for delivery of the critical service.
• Service continuity plans are developed using established standards, guidelines, and templates.
• Staff members are assigned to execute specific service continuity plans.
• Key contacts are identified in the service continuity plans.
• Service continuity plans are stored in a controlled manner and available to all those who need to know.
• Availability requirements such as recovery time objectives and recovery point objectives are established.
• Mechanisms (e.g., failsafe, load balancing, hot swap capabilities) are implemented to achieve resilience requirements in normal and adverse situations.

2. Service continuity plans are reviewed to resolve conflicts between plans.
• Plans are reviewed to identify and resolve conflicts.

3. Service continuity plans are tested to ensure they meet their stated objectives.
• Standards for testing service continuity plans have been implemented.
• A schedule for testing service continuity plans has been established.
• Service continuity plans are tested.
• Backup and storage procedures for high-value information assets are tested.
• Test results are compared with test objectives to identify needed improvements to service continuity plans.

4. Service continuity plans are executed and reviewed.
• Conditions have been identified that trigger the execution of the service continuity plan.
• The execution of service continuity plans is reviewed.
• Improvements are identified as a result of executing service continuity plans.

Risk Management (RM)

Purpose: To identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.

Risk management is a foundational activity for any organization and is practiced at all levels, from the executives down to individuals within business units. The CRR focuses on risks to cyber-dependent operations that have the potential to interrupt delivery of the critical service being examined. While the CRR focuses on *operational risk*, it is important to note that operational risk management requires a comprehensive approach to be effective.

The Risk Management domain comprises five goals and 13 practices:

1. A strategy for identifying, analyzing, and mitigating risks is developed.
• Sources of risk that can affect operations have been identified.
• Categories for risks have been established.
• A plan for managing operational risk has been established.
• The plan for managing operational risk has been communicated to stakeholders.

2. Risk tolerances are identified, and the focus of risk management activities is established.
• Impact areas, such as reputation, financial health, and regulatory compliance, have been identified.
• Impact areas have been prioritized to determine their relative importance.
• Risk tolerance parameters have been established for each impact area.
• Risk tolerance thresholds, which trigger action, are defined for each category of risk.

3. Risks are identified.
• Operational risks that could affect delivery of the critical service are identified.

4. Risks are analyzed and assigned a disposition.
• Risks are analyzed to determine potential impact to the critical service.
• A disposition (accept, transfer, mitigate, etc.) is assigned to identified risks.

5. Risks to assets and services are mitigated and controlled.
• Plans are developed for risks that the organization decides to mitigate.
• Identified risks are tracked to closure.

External Dependencies Management (EDM)

Purpose: To establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.

The outsourcing of services, development, and production has become a normal and routine part of operations for many organizations because outsourcing can engage specialized skills and equipment at a cost savings over internal options. The External Dependencies Management domain of the CRR presents a method for an organization to identify and prioritize those external dependencies and then focuses on managing and maintaining those dependencies.

The External Dependencies Management domain comprises five goals and 14 practices:

1. External dependencies are identified and prioritized to ensure operation of high- value services.
• Dependencies on external relationships that are critical to the service are identified.
• A process has been established for creating and maintaining a list of external dependencies.
• External dependencies are prioritized.

2. Risks due to external dependencies are identified and managed.
• Risks due to external dependencies are identified and managed.

3. Relationships with external entities are formally established and maintained.
• Resilience requirements of the critical service are established that apply specifically to each external dependency.
• These requirements are reviewed and updated.
• The ability of external entities to meet resilience requirements of the critical service are considered in the selection process.
• Resilience requirements are included in formal agreements with external entities.

4. Performance of external entities is managed.
• The performance of external entities is monitored against resilience requirements.
• The responsibility for monitoring external entity performance is assigned (as related to resilience requirements).
• Corrective actions are taken as necessary to address issues with external entity performance (as related to resilience requirements).
• Corrective actions are evaluated to ensure issues are remedied.

5. Dependencies on public services and infrastructure service providers are identified.
• Public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) are identified.
• Infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) are identified.

Training and Awareness (TA)

Purpose: The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.

Training and awareness focus on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization's operational cyber resilience requirements and goals are known and met. An organization plans for and conducts training and awareness activities that make staff members aware of their role in the organization's cyber resilience concerns and policies. Staff members also receive specific training to enable them to perform their roles in managing organizational cyber resilience.

The Training and Awareness domain comprises two goals and 11 practices:

1. Cybersecurity awareness and training programs are established.
• Cybersecurity awareness needs have been identified for the critical service.
• Required skills have been identified for specific roles (administrators, technicians, etc.) for the critical service.
• Skill gaps present in personnel responsible for cybersecurity are identified.
• Training needs have been identified.

2. Awareness and training activities are conducted.
• Cybersecurity awareness activities for the critical service are conducted.
• Cybersecurity training activities for the critical service are conducted.
• The effectiveness of the awareness and training programs is evaluated.
• Awareness and training activities are revised as needed.
• Privileged users are trained in their specific roles and responsibilities in support of the critical service.
• Senior executives are trained in their specific roles and responsibilities in support of the critical service.
• Physical and information security personnel are trained in their specific roles and responsibilities in support of the critical service.

Situational Awareness (SA)

Purpose: To actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.

Situational awareness activities are performed throughout the organization to provide timely and accurate information about the current state of operational processes. Activities must support communication with a variety of internal and external stakeholders to support the resilience requirements of the critical service.

The Situational Awareness domain comprises three goals and eight practices:

1. Threat monitoring is performed.
Responsibility for monitoring sources of threat information has been assigned.
Threat monitoring procedures have been implemented.
Resources have been assigned and trained to perform threat monitoring.

2. The requirements for communicating threat information are established.
Internal stakeholders (such as the critical service owner and incident management staff) to whom threat information must be communicated have been identified.
External stakeholders (such as emergency management personnel, regulators, and information sharing organizations) to whom threat information must be communicated have been identified.

3. Threat information is communicated.
Threat information is communicated to stakeholders.
Resources have been assigned authority and accountability for communicating threat information.
Resources have been trained with respect to their specific role in communicating threat information.

2.3 MIL Scale

The CRR uses Maturity Indicator Levels (MILs) to provide organizations with an approximation of the maturity of their practices in the 10 cybersecurity domains. The CRR's approach to maturity is based on an underlying capability maturity model, the CERT Resilience Management Model. [1] 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.

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.

---

[1] 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 the model are typically agreed on by the domain or discipline, which validates them through application and refinement.

The following example illustrates how MILs may be applied to the CRR Incident Management 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 perform incident management practices, but that it also plans the processes around incident management. In other words, among other requirements, the company has a documented policy to govern ownership and participation in incident management, and stakeholders know and understand their roles.

At the start of this fiscal year, a significant industry peer to SBM suffers a major theft of intellectual property because of a computer intrusion originating in another country. This incident causes SBM's executive leadership to place additional emphasis on incident management. They begin to provide oversight to incident management, ensure that staff are qualified, and dedicate adequate funding to incident management. They also evaluate and make decisions about the risks of deficiencies in the way that SBM does incident management. This level of maturity is roughly equivalent to MIL3 Managed *in the CRR.*

As part of a strategic plan to diversify and integrate the business, SBM is also acquiring a smaller company specializing in the direct sale of medical equipment to healthcare providers. The smaller company brings new risks, such as those associated with the electronic processing of customer billing and payment information. To integrate incident management with the new company, SBM

develops procedures and processes that managers in the new company can use to adapt their incident 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 CRR's highest maturity level, MIL5 Defined.

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 CRR 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 CRR questions.

MIL2 Planned
All specific practices in the CRR domain are not only performed but are 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.

3 CONDUCTING A CRR ASSESSMENT

Organizing for the Assessment

Identifying the Scope of the Assessment

It is expected that the facilitator will 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 CRR has a service-oriented approach, meaning that one of the foundational principles of the CRR is that an organization deploys its assets (people, information, technology, and facilities) to support specific operational missions (or services).

The CRR uses an identified critical service to frame the questions in the CRR. Therefore, you must select a critical service in your organization 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 CRR strives to identify how an organization aligns its cybersecurity management activities to the performance or production of its critical services. Often, an organizations 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 comprise 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 a CRR:

- 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?

What risks have been identified for the service?

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

Administering the CRR Assessment

The CRR 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 (IT operations, Business Continuity, Risk Management, and others as appropriate), are subject matter experts (SMEs) who provide insight relevant to the different CRR domains. The consensus 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 CRR Assessment requires the active participation of members of the organization who serve in a variety of roles. Table 2 summarizes the key roles involved in a typical assessment.

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 • deciding whether the organization should conduct a CRR 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 CRR Assessment. General responsibilities include • 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 CRR Assessment report • distributing the CRR 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 • 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 CRR's 10 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 objectives of this meeting include the following:

- Familiarize the sponsor and/or stakeholders with the CRR.
- Obtain executive support for 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 CRR Assessment to be successful, participants should be knowledgeable about the organization's cybersecurity practices in relation to both the selected critical service and the domains covered in the CRR. There should be SMEs familiar with how the organization operates in all 10 CRR domains (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

Asset Management	
Controls Management	
Configuration and Change Management	
Vulnerability Management	
Incident Management	
Service Continuity Management	
Risk Management	
External Dependencies Management	
Training and Awareness	
Situational Awareness	

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 six to eight 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 CRR Assessment to the organization, identify the business drivers for a cybersecurity effort, 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 CRR 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 CRR. The facilitator should ensure that the workshop participants are prepared and comfortable during the workshop.

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

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

Topic	Discussion
Organization’s vocabulary	Discussion of terms found in the CRR 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 set of activities performed by the organization and to describe those activities 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. The facilitator should emphasize that next steps will be based on the organization’s risks and maturity. The facilitator should also 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 Asset Management 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 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 CRR question guidance is useful in coming to this understanding.

3.1 Getting Started with the CRR Assessment in CSET®

System Requirements and Setup

Before starting, check that your system meets CSET requirements.

Local Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 6 GB free disk space
- 4 GB of RAM
- Microsoft Windows 10 or higher
- Microsoft .NET Core 5.0 Runtime (included in CSET installation)
- SQL Server 2019 Express LocalDB (included in CSET installation)

Enterprise Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 8 GB free disk space
- 4 GB of RAM
- Microsoft Windows Server 2016 Edition or higher recommended
- Microsoft .NET Framework 5.0 Runtime
- SQL Server 2019 or higher recommended
- Internet Information Server (IIS) or Kestrel

Please Note:

- For all platforms, it is recommended the user upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update web site to ensure the best compatibility and security. For additional help with CSET® installation, see the Installation Procedures section of the CSET General User Guide 11.0.

Downloading CSET

CSET 11.0 can be downloaded here. After installing the software, you will be prompted to enter CSET.

Accessing the CRR Assessment

1. Assessment Log Screen

Start by clicking the New Assessment  button at the top left corner of the screen. This screen also allows for importing and exporting of your assessment materials.

Figure 2: Start an Assessment Screen

2. Assessment Configuration Screen

The Assessment Configuration Screen collects assessment and facility information. After filling out the form, select Maturity Model from the Assessment Options section at the bottom of the page. Then click **Next**.

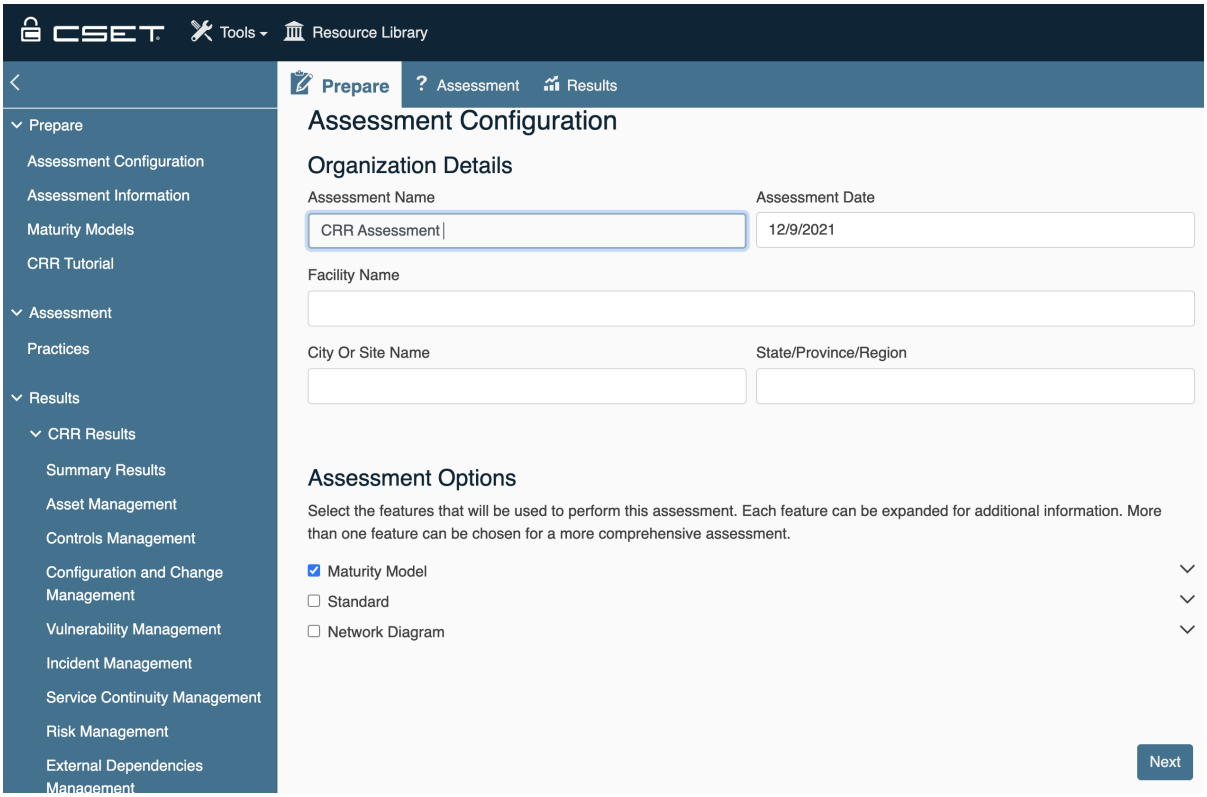

Figure 2.1: Assessment Configuration Screen

3. Assessment Information Screen

The Assessment Information screen collects demographic information. After filling out the form, click **Next**.

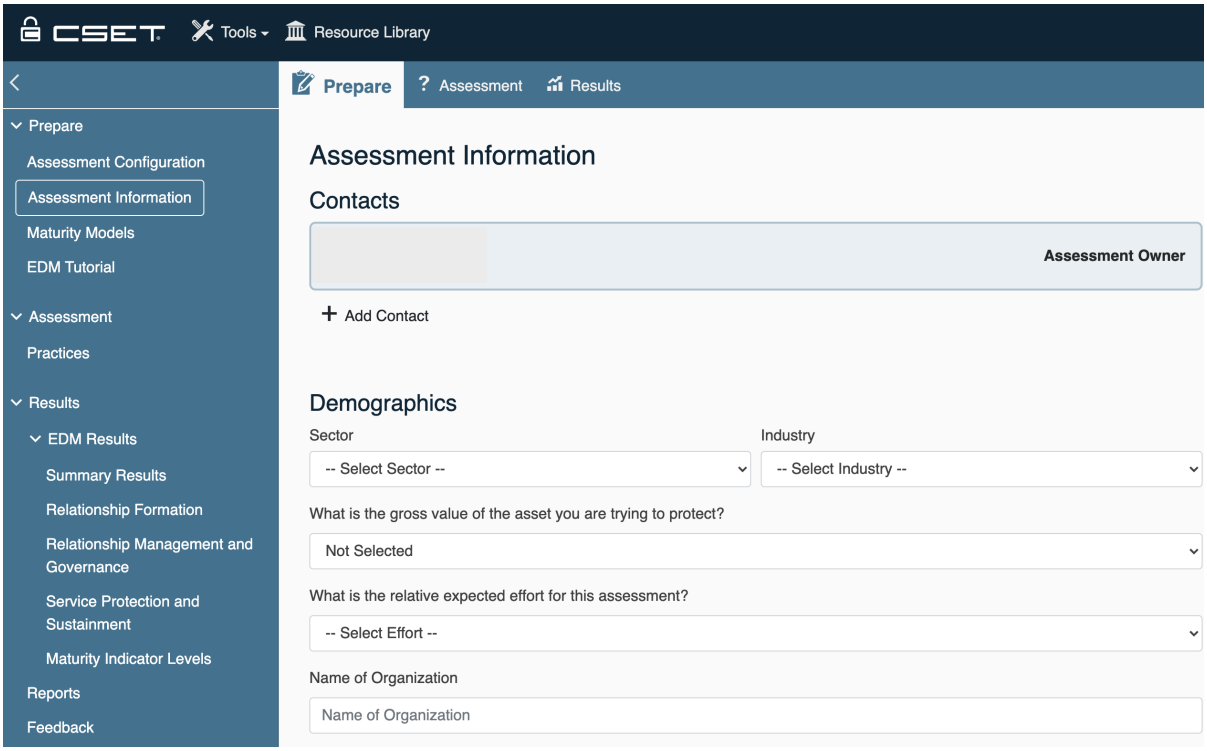

Figure 2.2: Assessment Information Screen

4. Maturity Model Selection Screen

The next step in the menu sidebar is the Maturity Models selection screen. To access the CRR Assessment, click the Maturity Models selection from the sidebar menu. The CRR Assessment is located in the Maturity Model section of the CSET® tool. Click to highlight the CRR Assessment and select, then click **Next.** After clicking next, the CRR Tutorial will appear.

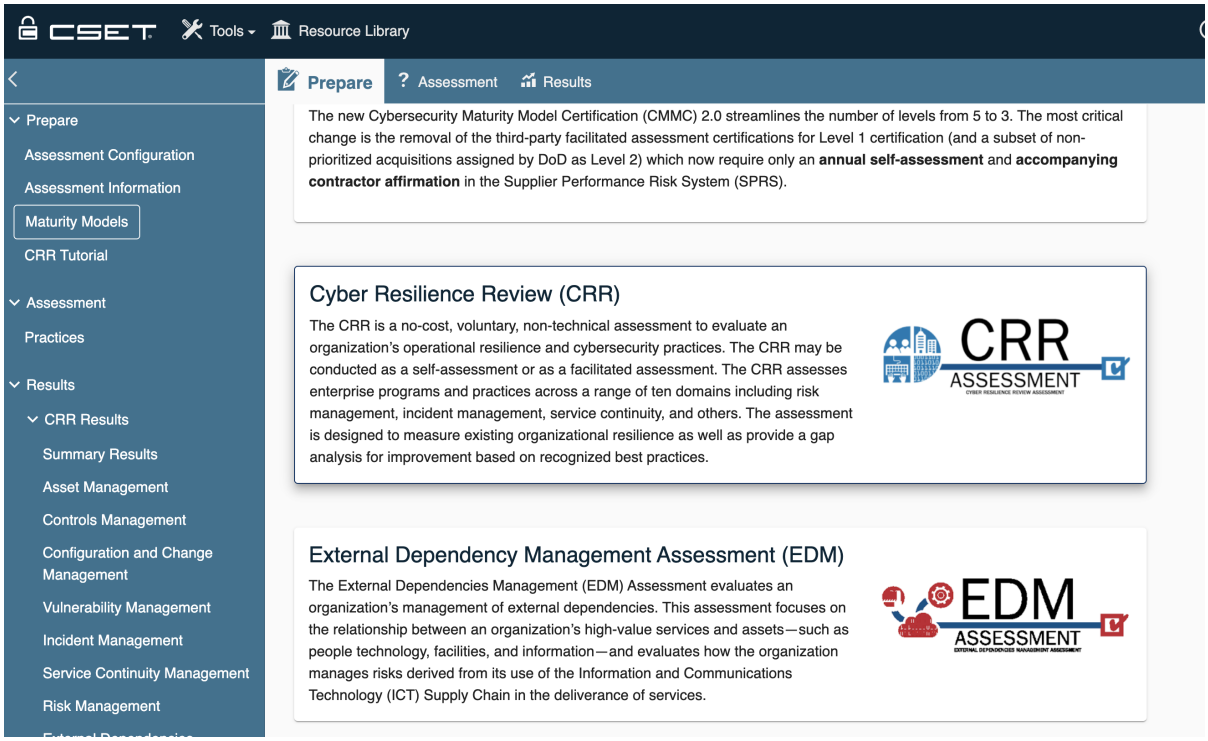

Figure 2.3: Maturity Model Selection Screen

5. CRR Tutorial

Take a moment to read through the tutorial page for CRR Assessment background information and key steps to getting started with your assessment.

The CSET® CRR Assessment provides the following:

- CRR question set with guidance and references
  - Feedback mechanism for each question
  - Comments field for notes recorded specific to each question (these notes are private to the facilitator)
  - Domain-specific remarks field for inserting notes into the corresponding report section (these notes appear verbatim in the report)
  - Artifacts / documents attachment function
- Compilation of answers and results specific to each domain
- Automated scoring
- Multiple reports with Business Confidential / CUI marking options, detailed results, deficiencies, and suggested options for consideration offered in both HTML and PDF formats.

The CRR Assessment Tutorial starts in Section 3.2

.

3.2 Tutorial: Using the CSET® CRR Assessment Software

Practice Questions Structure

Each practice question contains a 3-point response scale to evaluate the degree to which the organization has implemented each practice. Each question has three possible answers: “Yes”, “Incomplete”, and “No”:

• **Yes** – the organization fully performs the activity specified in the question.

• **Incomplete** – the organization partially performs the activity

• **No** – the organization does not perform the activity at all.

Mark for Review: To the right of the of the three-point response scale is the Flag icon which can be used to flag a practice for review.

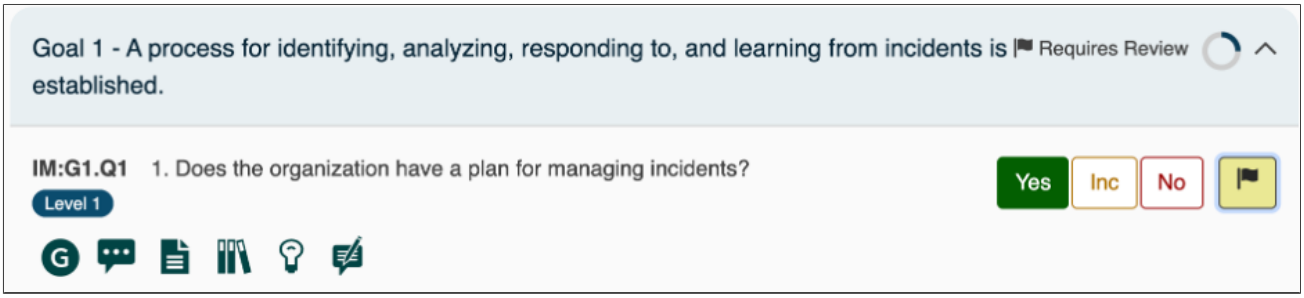

Figure 3: Assessment Question Structure

Supplemental Guidance: To aid the facilitator, each question is supported by guidance. The guidance should be referred to for background, possible examples, and artifacts, **and for criteria that defines the requirements for a “Yes” and an “Incomplete” answer**. The guidance is engaged by selecting the Guidance Icon containing the letter “G” located below the question.

Comments: Selecting this icon will display a text box that may be used to make comments regarding the question. For example, a facilitator, for future reference may make

a note as to why an answer was marked incomplete vs. no. Note, these comments are not included in the official report and are meant to be private to the facilitator.


Artifacts / Documents: Easily associate, track, and store artifacts, and other supporting documents throughout the assessment.


References: Selecting the References Icon will display the Options for Consideration and reference material associated with the particular question. The Options for Consideration are normally found in the report but are also made available to the facilitator while performing the assessment. These options outline general guidelines or activities and the associated sources that can be used to improve the organization's cybersecurity practices and the resilience of the critical service assessed.


Observations: Selecting this icon will pop up an observation details dialog box used to capture information about an issue associated with the particular practice along with its importance, resolution date, etc.


Feedback: Used to provide feedback regarding the question to CISA. For example, a user may comment that the question language is too complex and suggest alternate wording. Note: A red dot indicator will appear when feedback has been recorded.

Domain Remarks Text Box

At the end of each domain a Domain Remarks text box is available to the user. 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.

For example, if an improvement effort is already underway to address some of the practices in a particular domain, it can be detailed here to make it part of the official report. **Since this text is copied verbatim into the report a user should use discretion in their commentary.**

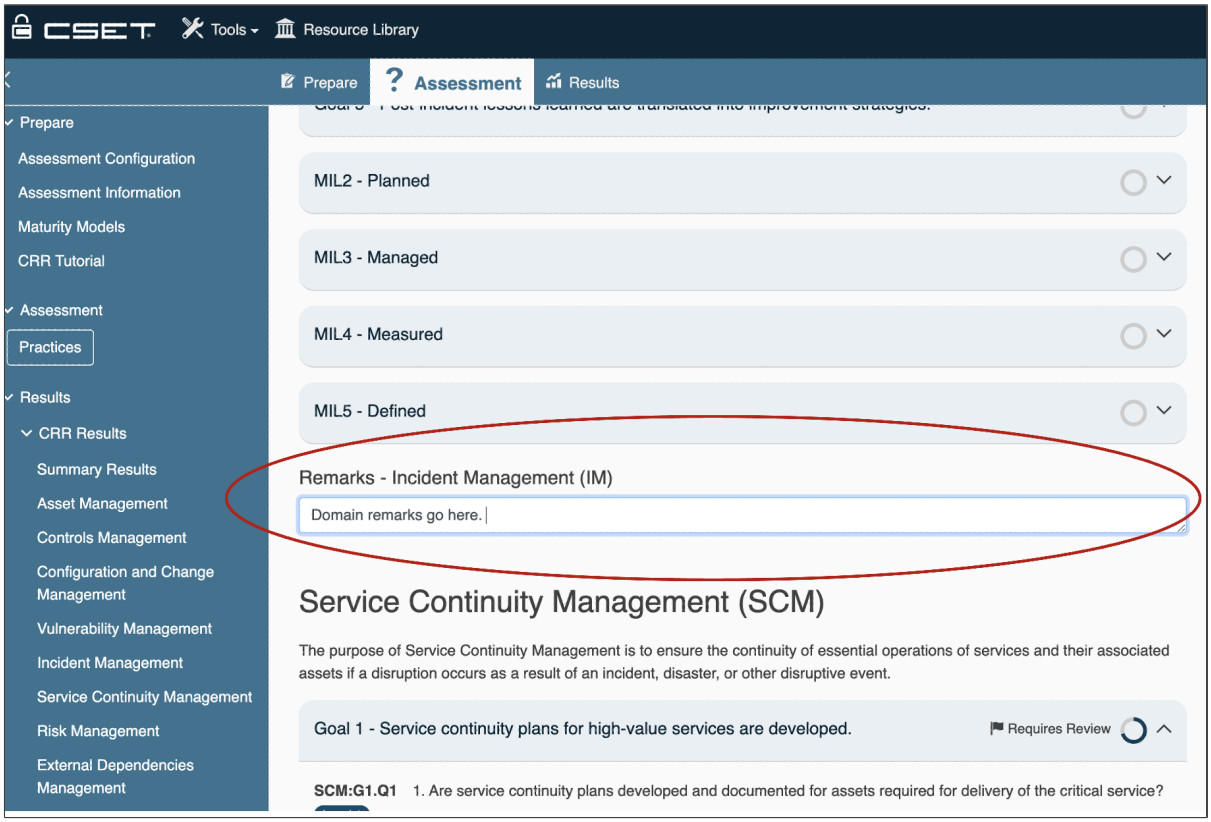

Figure 4: Domain Remarks Field

Asset Types

The CRR divides assets into four categories: **People, Information, Technology, and Facilities**.

The four asset types are:

• **People** - the staff (both internal and external to the organization) such as people that support data centers or otherwise use information and communications technology to operate and monitor the service.

• **Information** - account information, technology asset configuration files, operational data, customer information and other information necessary for the delivery of the service.

• **Technology** – computers (hardware), software, control systems, or other technology including external information systems used by the organization to deliver the service.

• **Facilities** – offices buildings, data centers and other physical structures supporting the delivery of the service.

See the Asset Types example in Figure 5.

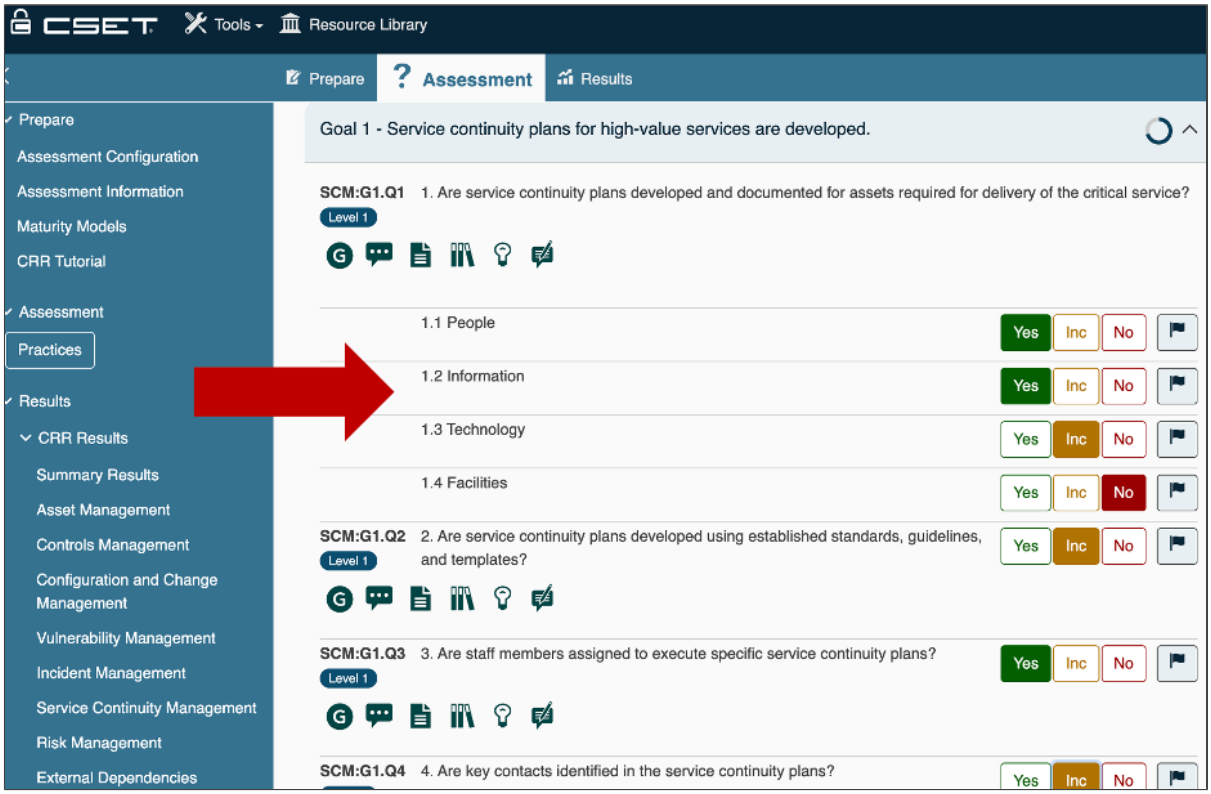

Figure 5: Asset Types

4 CRR Assessment Results and Report

CSET® offers the CRR Report in both HTML and PDF format.

Results

A user can view their **CRR Summary** and **domain-specific** results from the sidebar menu on the left side of the screen.

Reports

To view the reports, click the Reports tab on the sidebar menu and choose your desired confidentiality level (**Business Confidential / CUI selection is available for the CRR Report only**).

From the reports menu, a user can also view their **CRR Deficiency Report** and **CRR Comments and Marked for Review** reports.

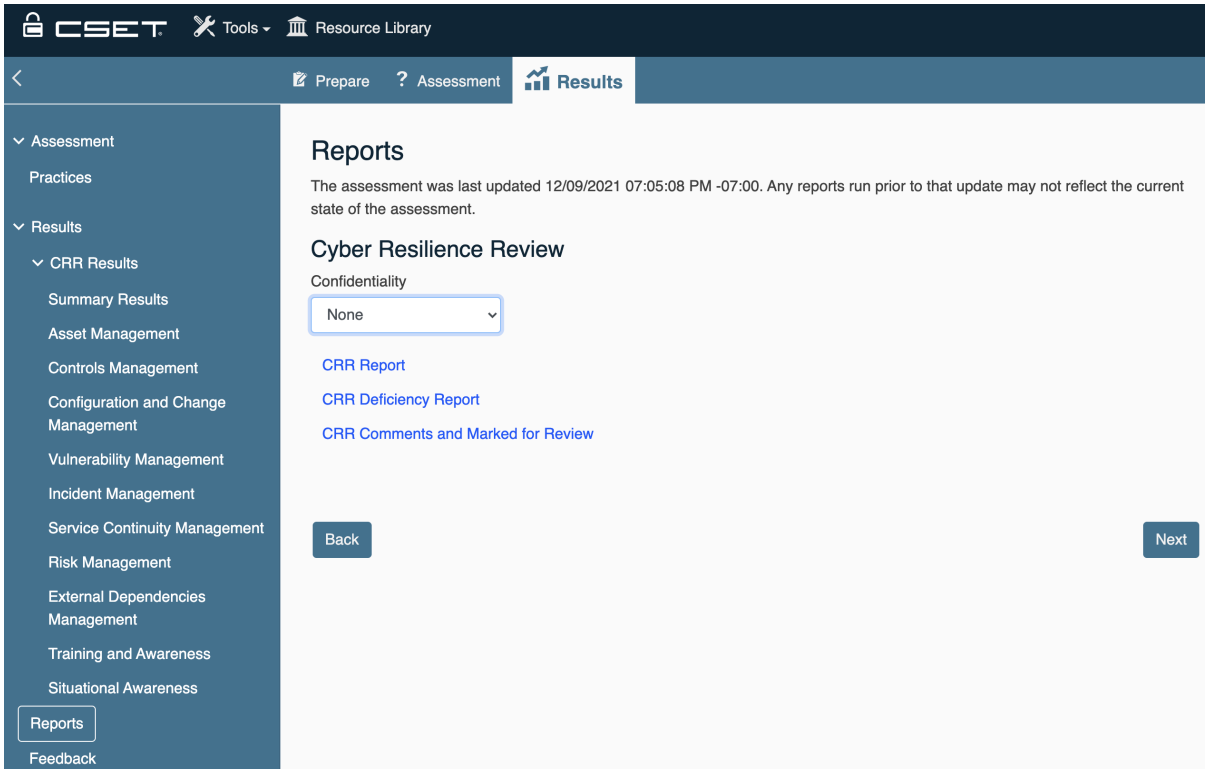

Figure 6: Reports Screen

Generating the CRR Report

Reports can be downloaded in PDF format from the top of the sidebar menu.

Figure 7: CRR Report Menu with Download Report (PDF) Function

4.1 CRR 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 domain is achieved at MIL1 if all the goals in the domain are achieved.
4. A domain 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 CRR 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 CRR 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 10, is useful for identifying areas for improvement.

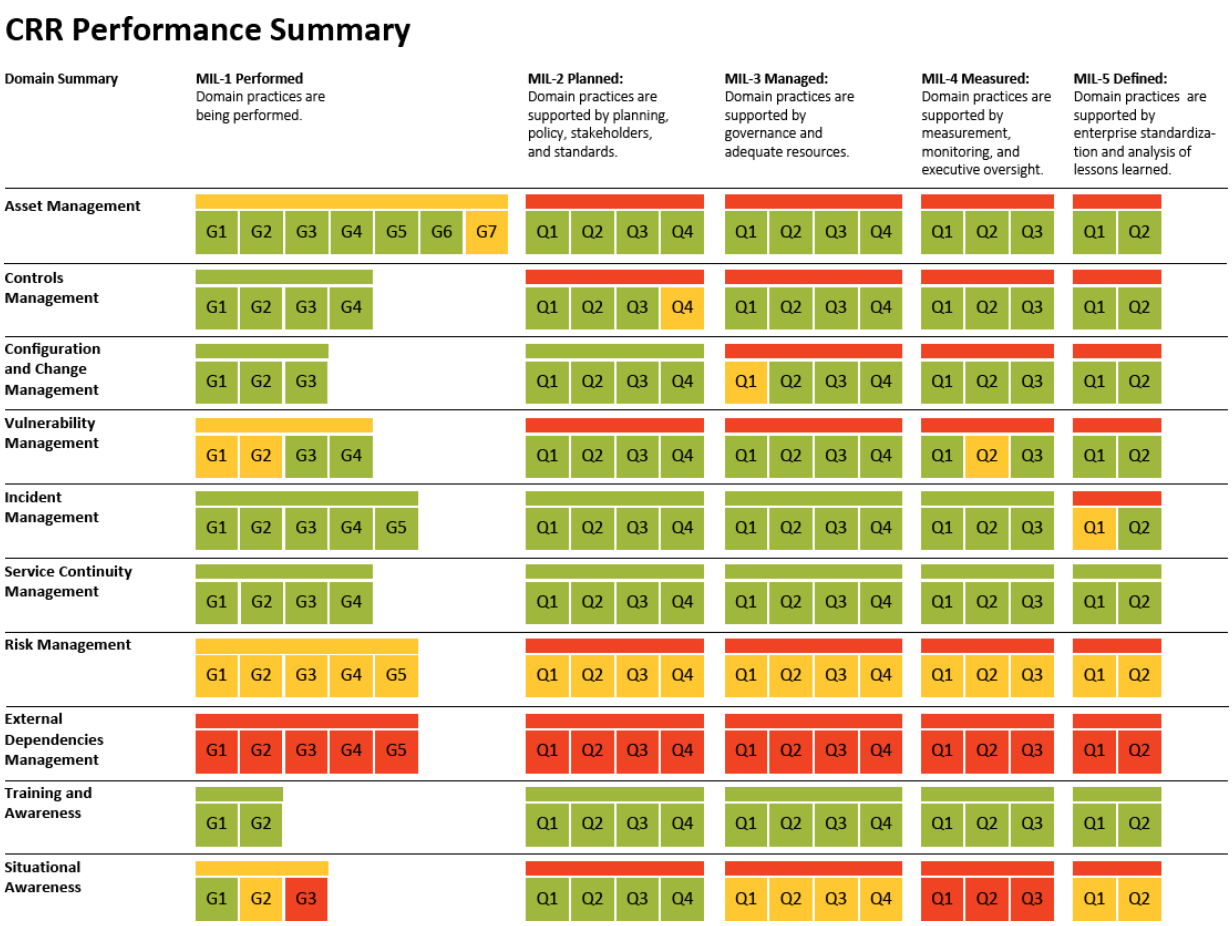

Figure 8: CRR Performance Summary

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.

Figure 9: A Sampling of Individual Domains

Figure 9 shows that MIL1 is not achieved in Asset Management, Risk Management, External Dependencies Management, or Situational Awareness. 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 External Dependencies Management 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 those related practices first.

Individual domain reports, as shown in Figure 10 and Figure 11, provide question-level detail to help organizations focus on specific practices for improvement.

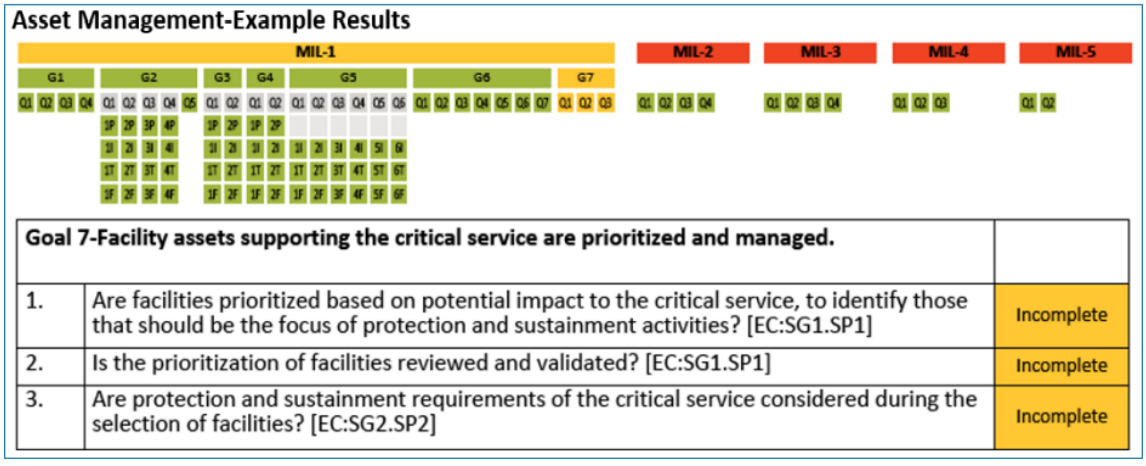

Figure 10: Asset Management Individual Domain Report

In the Asset Management scenario shown in Figure 10, the organization may benefit from focusing on the prioritization, review, and resilience requirements of facilities to advance from the current MIL1 state all the way to MIL5, as all other practices are currently performed.

Alternatively, the organization's risk analysis may indicate that the practices in Goal 7 are not a priority, possibly because there is only one facility. The organization should focus on improvements in areas of highest risk rather than simply trying to achieve a higher MIL for its own sake.

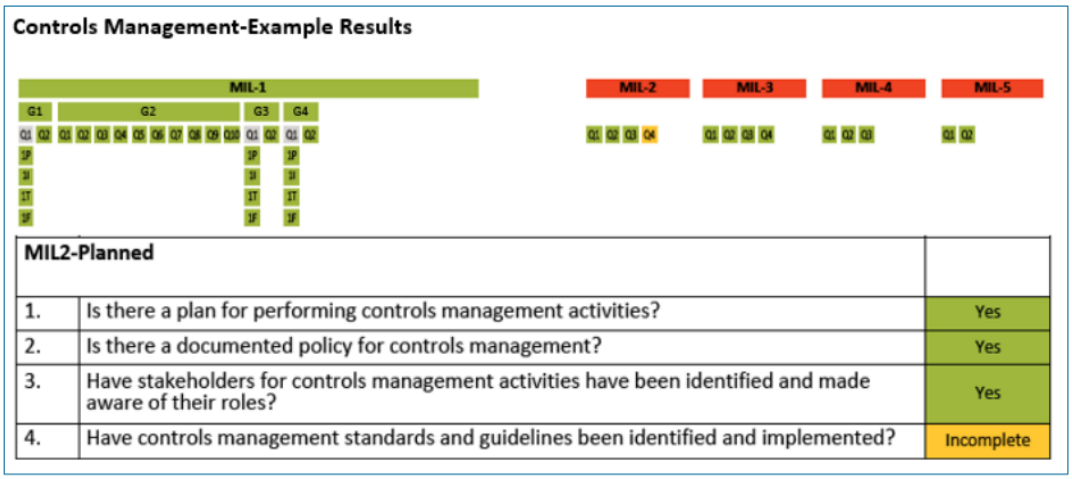

Figure 11: Controls Management Individual Domain Report

In the Controls Management scenario shown in Figure 11, all that is needed to achieve MIL2 is to implement standards and guidelines for controls management activities. This may be a relatively simple task. The organization would then achieve MIL5, as all other practices are performed.

However, an inspection of the Configuration and Change Management, Training and Awareness, and Incident Management domains reveals that the organization is already performing at higher MIL levels, so their efforts may be better focused on addressing the deficient domains that have not achieved even a basic level of MIL1.

The CRR MIL1 Performance Summary shown in Figure 12 provides an in-depth summary of MIL1 goals and practices for each CRR 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 CRR.

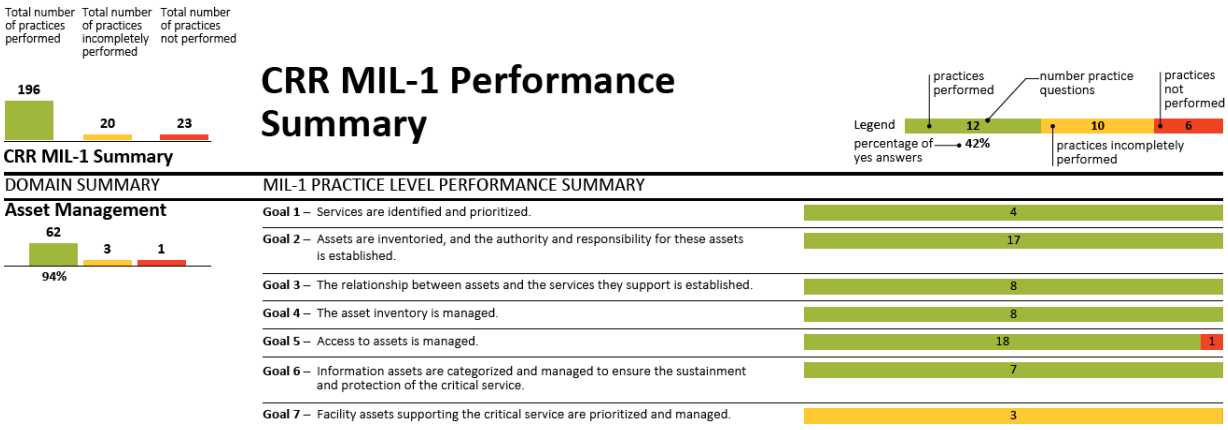

Figure 12: CRR MIL-1 Performance Summary – Asset Management

Similarly, The CRR MIL1 Performance depiction shown in Figure 13 provides a finer level of operational detail. In the Vulnerability Management scenario presented in Figure 13, the organization can determine that facility assets are not managed as well as other asset types. This view can be used to aid in identifying discrepancies with how assets are being managed.

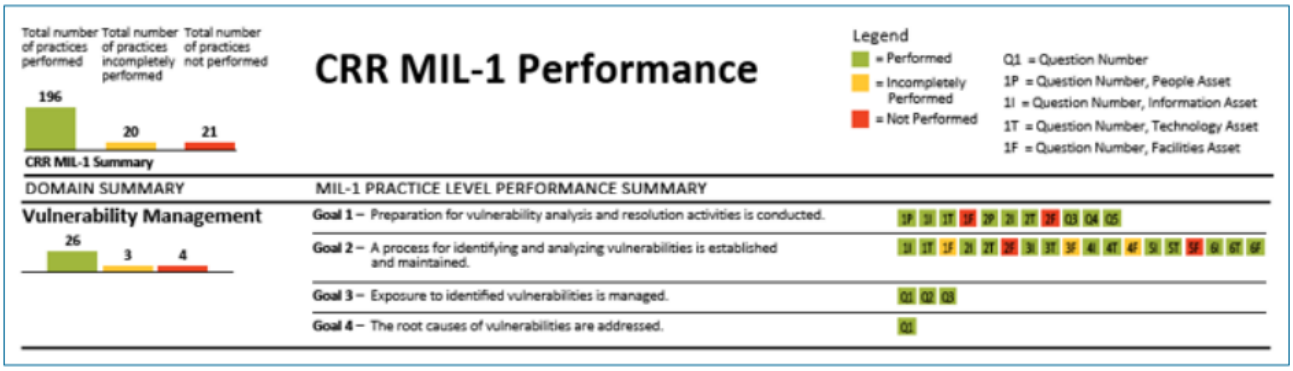

Figure 13: CRR MIL-1 Performance – Vulnerability Management

Additionally, the CRR Performance depiction shown in Figure 14 and located in Appendix A of the report provides a detailed operational view of the entire CRR.

Figure 14: CRR Performance View

Figure 15: Summary of CRR Results and Figure 16: Percentage of Practices Completed by Domain should be used in conjunction with each other when examining results. To illustrate this point, refer to the Asset Management portion of each depiction.

While Figure 15 shows that MIL1 was not achieved for the Asset Management domain, Figure 16, which shows the Percentage of Practices Completed by Domain graph (available in both the CRR Results and CRR Reports sections) reflects that 95% of the Asset Management domain practices are performed. It is important to remember that MILs are cumulative and that all practices at all lower MILs must be performed in order to achieve a higher MIL.

Summary of CRR Results

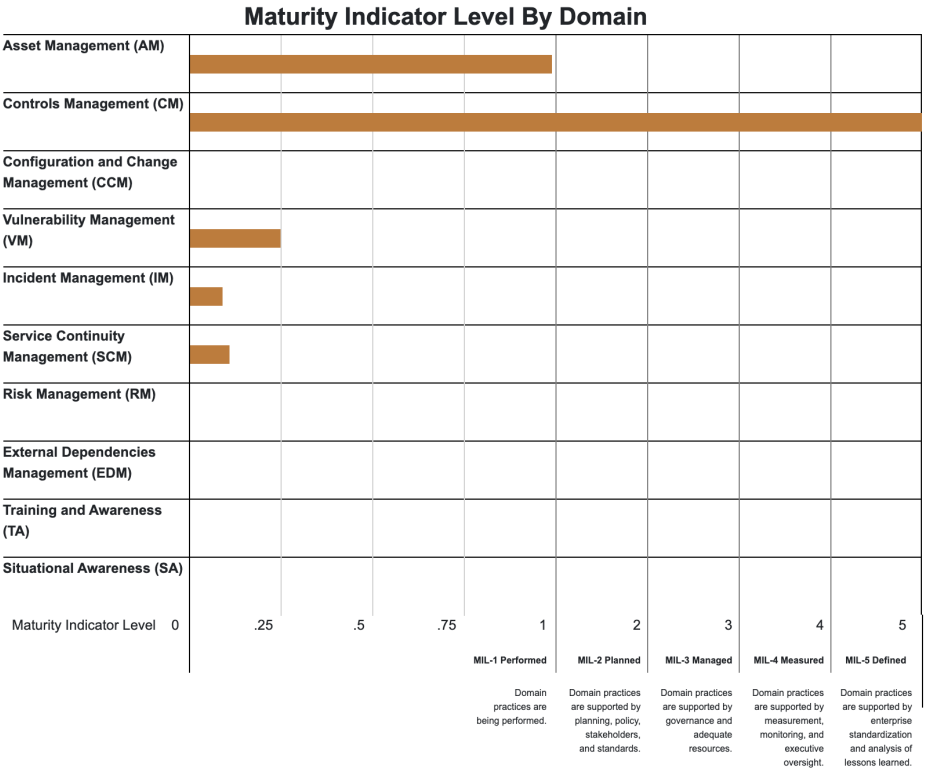

Figure 15: Summary of CRR Results

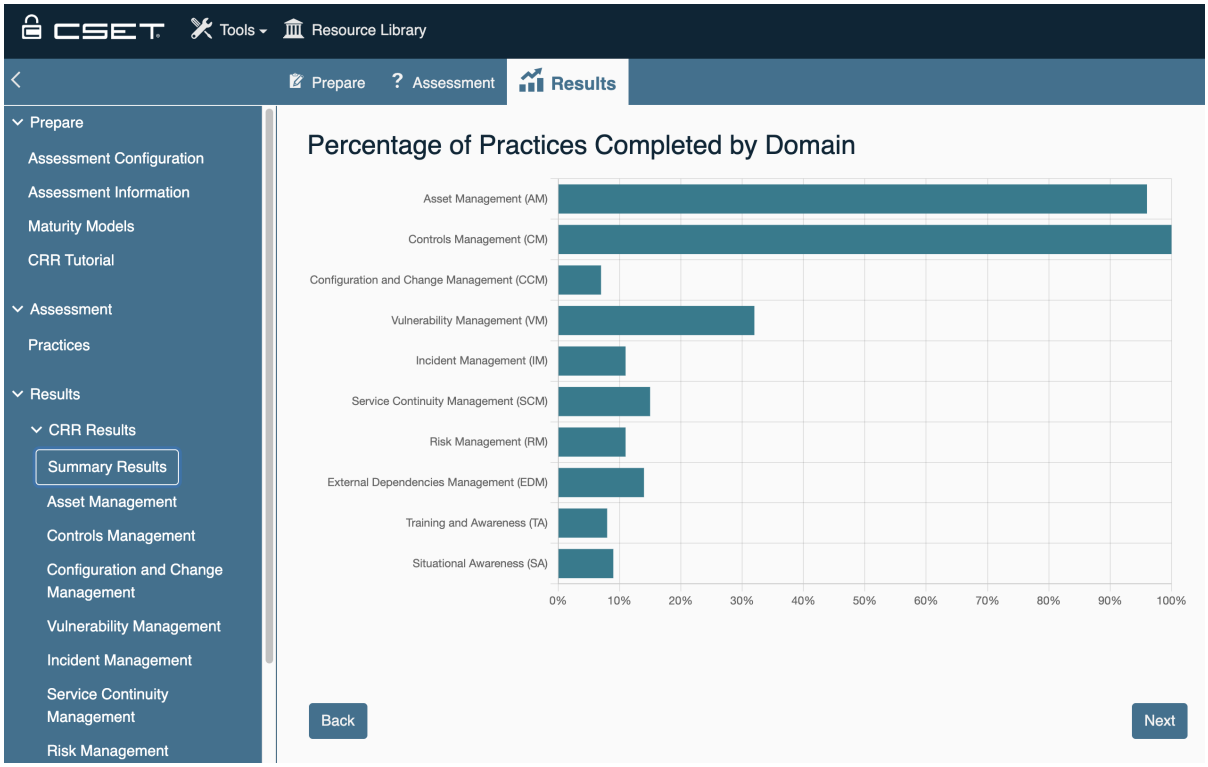

Figure 16: Percentage of Practices Completed by Domain

NIST Cybersecurity Framework Scoring Depictions

The CRR Assessment also enables an organization to assess its capabilities relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Each CRR practice has been mapped to the applicable categories and subcategories of the NIST CSF.

Figure 17 displays the organization's results by function and category. An organization can use the summary of results to focus on prioritizing categories it chooses to improve. For example, while the organization is performing 63% of the practices that comprise the Identify Function, the results also show that the organization is incompletely performing all the practices that relate to the Risk Management Strategy category. Therefore, the organization may choose to prioritize the implementation of practices that would lead to the improvement of the Risk Management Strategy category.

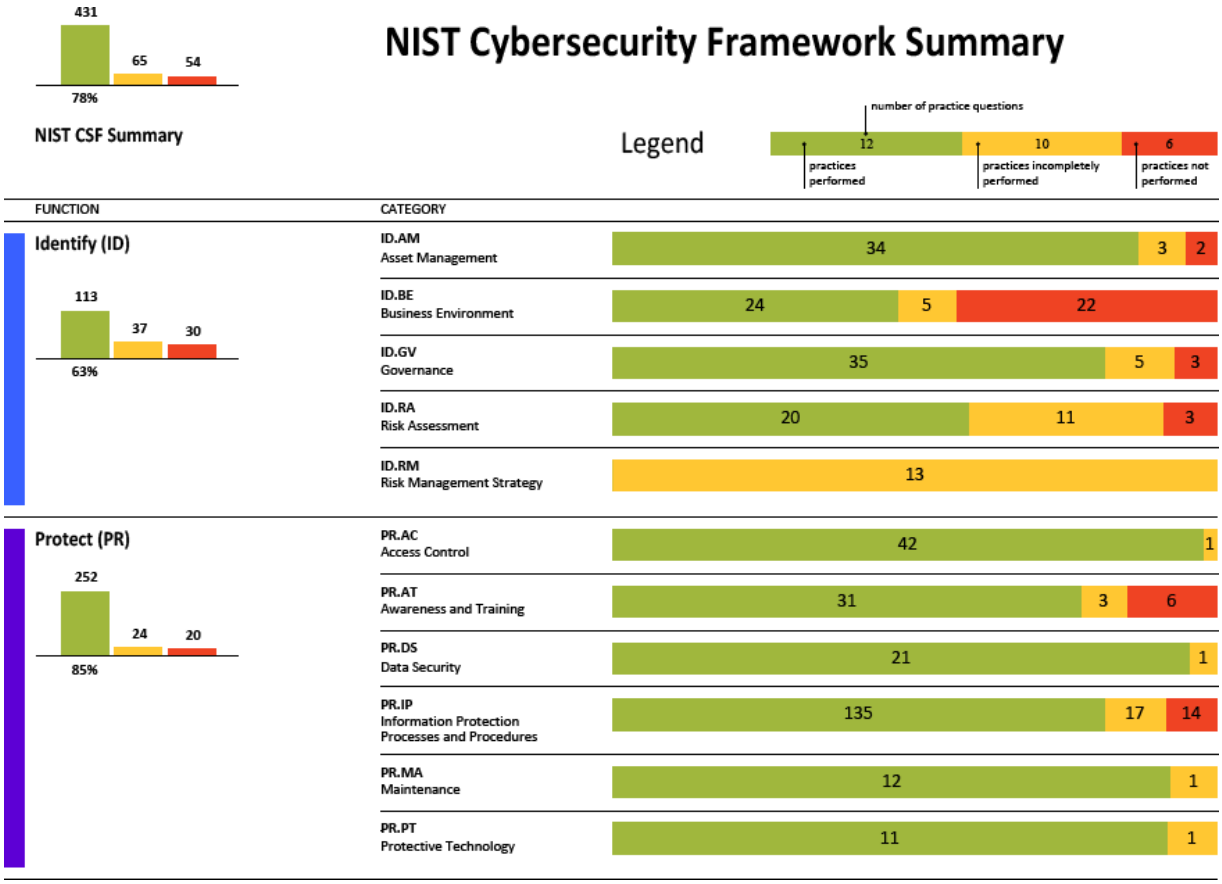

Figure 17: NIST Cybersecurity Framework Summary

Additionally, there are several NIST CSF depictions located in Appendix A that show a more detailed view of the NIST CSF Categories and Subcategories. Figure 18 depicts the performance of the Identify Function Asset Management (AM) Category based on the organization's CRR responses.

It is important to note that the ID.AM Category has 19 unique CRR practices mapped to it. This does not represent a roll up of all the subcategory practices depicted on the right side of the graphic. There are 19 CRR practices mapped to the ID.AM category because they represent practices that an organization should be performing as part of an Asset Management Program but there are no specific AM subcategories that address these practices directly

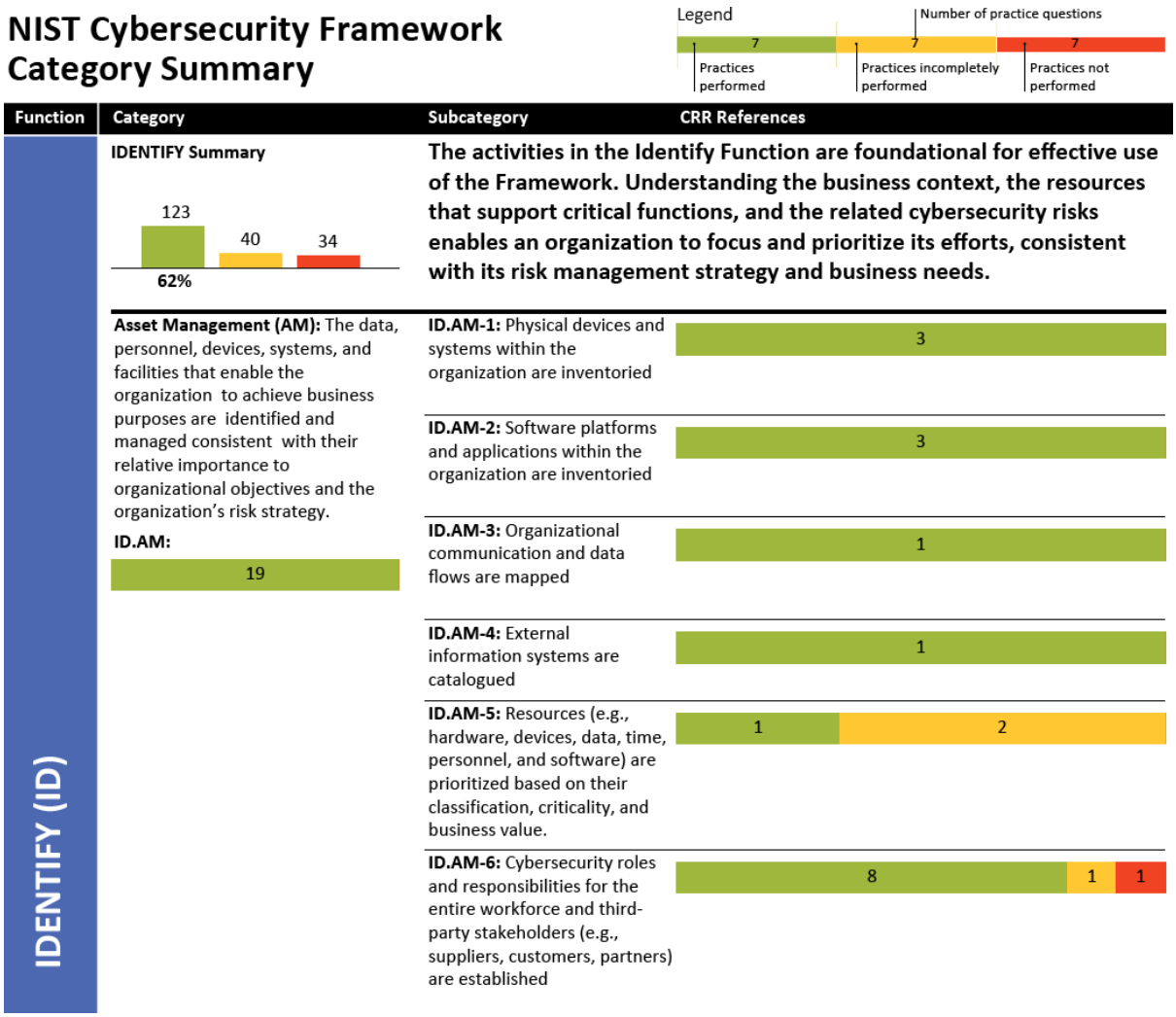

Figure 18: NIST Cybersecurity Framework Category Summary

An organization can also use the NIST Cybersecurity Framework Category Performance depiction (Figure 19) to view the organization's coverage of the NIST CSF Categories and Subcategories and to track its improvement efforts. The depiction acts a dynamic crosswalk for the user and can quickly be referenced to see which CRR practices are mapped to specific CSF categories and subcategories.

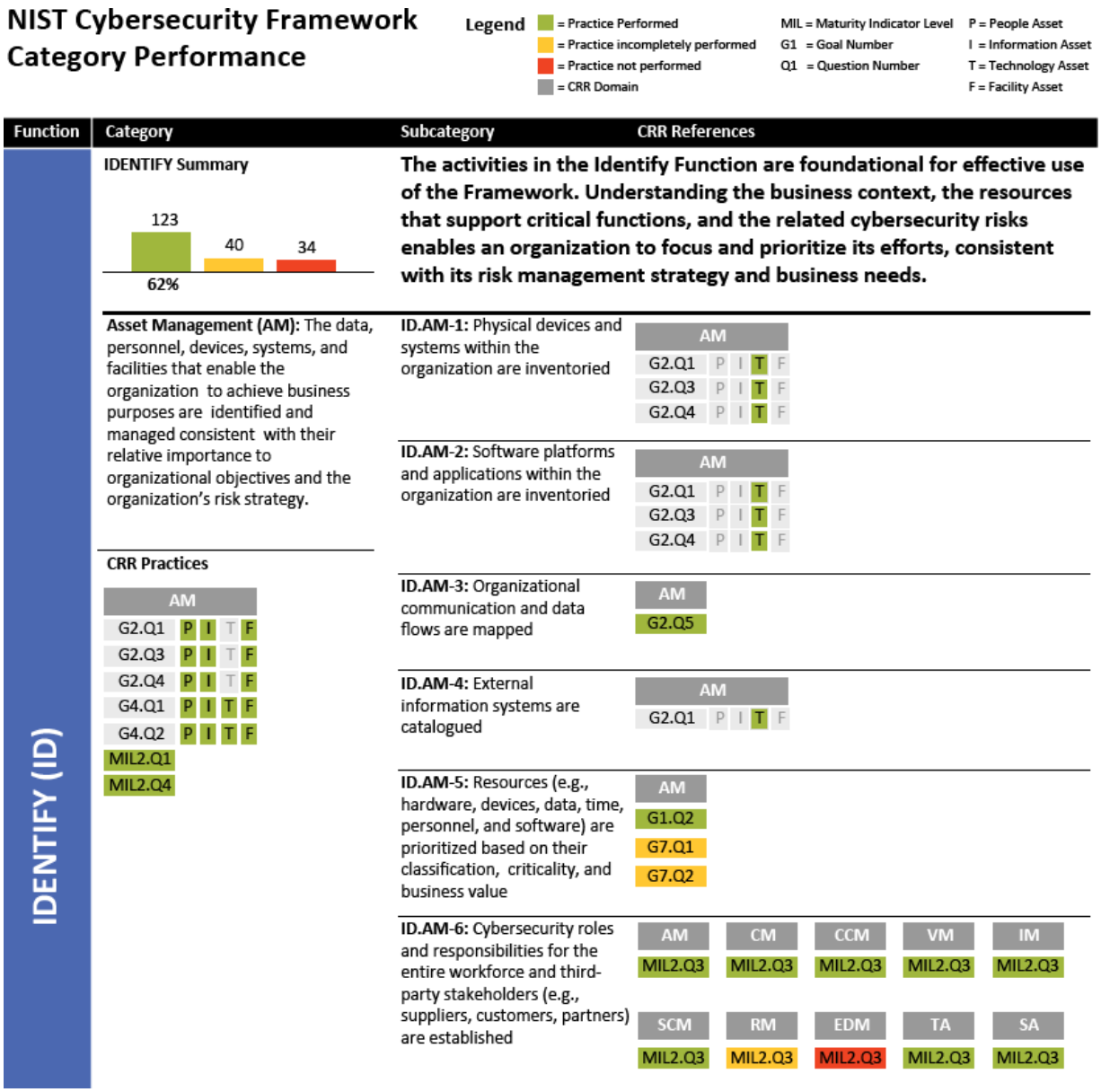

Figure 19: NIST Cybersecurity Framework Category Performance

Options for Consideration

The CRR 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 (Figure 20).

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[SC:SG2.SP1]** Identify the organization's high-value services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional References:** • Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 15-18 • NIST CSF References: ID.BE	

Figure 20: Options 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 20, the CERT-RMM reference for Question 1 (Q1) is to Service Continuity: Specific Goal 2.Specific Practice 1.

4.3 Identify Gaps

The CRR Assessment evaluates maturity across 10 domains of cybersecurity 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

Table 5 gives a more detailed description of the process improvement activities.

Table 5: Recommended Process for Using Results

	Inputs	Activities	Outputs
Perform Evaluation	1. CRR Assessment 2. Organizational policies and procedures 3. Understanding of current cybersecurity management and operations	1. Conduct the CRR Assessment	1. CRR Assessment Report
Analyze Identified Gaps	1. CRR Assessment Report 2. Understanding the organization's objectives with respect to the critical service and its impact on critical infrastructure	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	1. List of gaps and potential impact
Prioritize and Plan	1. List of gaps and potential impact 2. Understanding of organizational constraints (e.g., resources, legislation)	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	1. Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Monitor and measure implementation progress against plan 2. Reevaluate periodically and in response to major changes in the risk environment	1. Improvement plan tracking data

The CRR does not prescribe that organizations should reach specific MILs. As described above, the organization must determine the appropriate plan of action for improvement based on organizational objectives and risk environment.

5 MAKING IMPROVEMENTS

The CRR does not prescribe the achievement of specific MILs for organizations in any particular sector. The CRR Assessment Report provides an organization with information on its current level of cybersecurity capabilities in each of the 10 CRR domains and can be used as a baseline for initiating a data-driven process improvement project, as depicted in Figure 21.

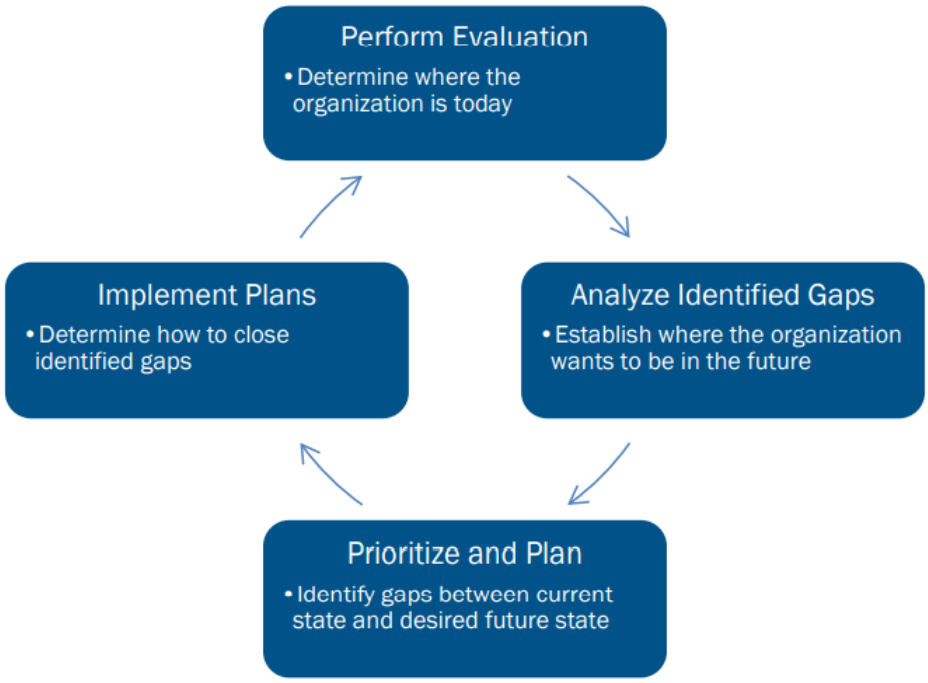

Figure 21: Steps in a Typical Process Improvement Activity

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

5.1 Analyze Identified Gaps

The CRR 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 CRR.

It probably 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 CRR Assessment to identify a desired target, is often adopted by organizations that are new to the CRR 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 CRR practices.

Setting a Target: Method 1

In this approach, an organization uses the results of a completed CRR assessment to jump-start the identification of its target state. The organization begins by walking through its scores in each domain of the CRR 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 needs to be performed to meet the organization's business and cybersecurity objectives.
3. If the practice needs to 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 10 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 CRR 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 needs to 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 10 model domains.

Once this review is complete, the organization will have a documented list of practices that it believes it needs to 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 plans have been developed and implemented 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 CRR Assessment Package can track progress toward the organization's desired capability profile.

6 SUMMARY

This document describes the Cyber Resilience Review (CRR) architecture and provides detailed descriptions of the 10 CRR domains and six Maturity Indicator Levels (MILs). This document also contains information about how to prepare for a CRR 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 CRR Assessment Report.

The CRR 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 CRR goals and practices is included in the CRR Assessment Kit.
For additional assistance, the facilitator and other participants can contact the Department of Homeland Security (DHS) at cyberadvisor@hq.dhs.gov.

APPENDIX A: PROCESS CHECKLIST

CRR Assessment Checklist

Purpose: To guide the CRR Assessment process

Time	Item	Description	Completed
Four weeks prior to assessment workshop	Preparation Meeting	Hold a preparation meeting. -Answer organizational questions. Establish the scope of the assessment. –Identify participants. –Schedule the assessment workshop.	
Two weeks prior to assessment workshop	Facilities	Ensure that facilities have been set up correctly. –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 the latest version of Adobe Reader or Adobe Acrobat.	
	Catering	Confirm catering, as applicable.	
One week prior to assessment workshop	Availability	Confirm that all participants are available and committed to attend the workshop.	

Name	Title	Role (CRR Domain)

Time	Item	Description	

	Sponsor	Confirm that the sponsor is prepared to deliver opening remarks or has delegated this responsibility to another executive.	
After the assessment workshop	Interpreting CRR Assessment Report	Examine the CRR Assessment Report and answer the following questions: 1. What are the overall strengths and weaknesses (see the Overall CRR Results chart in the report)? – What domains have not achieved at least MIL1? – What domains have achieved MIL3 or above? – What domains show the highest level of achievement? 2. What domain practices should the organization focus on (see the detailed domain sections of the report)? – 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. –Review each domain and identify what level of achievement is desired in the next three to five years. 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 CRR Assessment Report) to the future state (where the organization wants to be in the next three to five years). 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 need to be performed to achieve the future state. Consider 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 -the availability of resources to implement the practices A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed. Create a plan to achieve the future state, using the prioritized list of identified practices that need to be implemented.	
	Implementing plan	Implement the plan. -Assign resources to implement the plan. -Periodically conduct assessments to measure progress. -Manage progress against the plan. -Re-plan as necessary.	

APPENDIX B: CRR GLOSSARY/TERMS

asset (organizational asset)	Something of value to an organization; typically, people, information, technology, and facilities that the critical services rely on. One of the foundational principles of the CRR design is the idea that an organization deploys its assets (i.e., people, information, technology, and facilities) to support specific operational missions. Failure in any of these assets may result in a cascading impact on related business processes, services, and the organization's mission.	Adapted from CERT-RMM
Asset Management (AM)	A domain of practice within the CRR. The purpose of asset management is to identify, document, and manage assets during their lifecycle to ensure sustained productivity to support critical services.	CRR
awareness	Focusing the attention of, creating cognizance in, and acculturating people throughout the organization to resilience issues, concerns, policies, plans, and practices.	CERT-RMM
change control (change management)	A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption.	CERT-RMM
Configuration and Change Management (CCM)	A domain of practice within the CRR. The purpose of configuration and change management is to establish processes to ensure the integrity of assets using configuration and change control audits.	CRR
configuration management	A collection of activities focused on establishing and maintaining the integrity of assets through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their lifecycle.	NIST SP 800-128
controls	The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards.	CERT-RMM

Term	Definition	Source
Controls Management (CM)	A domain of practice within the CRR. The purpose of controls management is to identify, analyze, and manage controls in a critical service's operating environment.	CRR

critical service	A set of activities an organization carries out in the performance of a duty or in the production of a product that is so critical to the organization's success that its disruption would severely impact continued operations or success in meeting the organization's mission.	CRR
data leak	The intentional or unintentional release of information to an untrusted environment.	NIST SP 800-53
data at rest	Data at rest is information located on storage devices that are components of information systems.	NIST SP 800-53
data in transit	Data in transit is information that is being transmitted on both internal and external networks.	NIST SP 800-53
defined practice	A practice that is planned and executed in accordance with policy.	Adapted from CERT-RMM
domain	In the context of the CRR structure, a domain is a logical grouping of cybersecurity practices that contribute to the cyber resilience of an organization.	CRR
enterprise	The largest (i.e., highest level) organizational entity to which the organization participating in the CRR survey belongs. For some participants, the organization taking the survey is the enterprise itself. See *organization*.	Adapted from SGMM v1.1 Glossary
event	One or more occurrences that affect organizational assets and have the potential to disrupt operations.	CERT-RMM
External Dependencies Management (EDM)	A domain of practice within the CRR. The purpose of external dependencies management is to establish processes to manage an appropriate level of IT, security, contractual, and organizational controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.	CRR
external dependency	An external dependency exists when an external entity has access to, control of, ownership in, possession of, responsibility for, or defined obligations related to one or more assets or services of the organization.	CERT-RMM

Term	Definition	Source
external entity	An individual, business, or business unit (such as a customer, a contractor, or even another group within the same enterprise) that is external to and in a supporting or influencing relationship with the organization that is using the CRR.	Adapted from CERT-RMM
facility	Any tangible and physical asset that is part of the organization's physical plant. Facilities include office buildings, warehouses, data centers, and other physical structures.	CERT-RMM

governance	An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT-RMM
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts.	Adapted from CERT-RMM
Incident Management (IM)	A domain of practice within the CRR. The purpose of incident management is to establish processes to identify and analyze IT events, detect cybersecurity incidents, and determine an organizational response.	CRR
information asset	Information or data that is of value to the organization, including diverse information such as operational data, intellectual property, customer information, and contracts.	Adapted from CERT-RMM
least functionality	Refers to the configuration of information systems to provide only essential capabilities and prohibit or restrict the use of unnecessary functions, ports, protocols, services, etc.	NIST SP 800-53
least privilege	Least privilege is employed to ensure users and processes operate at privilege levels no higher than necessary.	NIST SP 800-53

Term	Definition	Source
Maturity Indicator Level (MIL)	The MIL scale measures the level of process institutionalization and describes attributes indicative of mature capabilities. Higher degrees of institutionalization translate to more stable processes that produce consistent results over time and that are retained during times of operational stress.	CRR
mobile code	Mobile code is software transferred between systems and executed on a local system without explicit installation by the recipient. Mobile code technologies include, Java and JavaScript, ActiveX, PDFs, Shockwave movies, Flash animations.	NIST SP 800-53
monitoring	Collecting, recording, and distributing information about the behavior and activities of systems and persons	Adapted from CERT-RMM

	to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	(Monitoring and Risk Management)
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.	Adapted from CERT-RMM
operational risk taxonomy	The collection and cataloging of common operational risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line of business if operational assets and services are affected by them.	CERT-RMM
organization	An administrative structure in which people collectively manage one or more services as a whole and whose services share a senior manager and operate under the same policies. May consist of many organizations in many locations with different customers.	CERT-RMM
people	All staff, both internal and external to the organization, and all managers employed in some manner by the organization to perform a role or fulfill a responsibility that contributes to meeting the organization's goals and objectives.	CERT-RMM
plan	A detailed formulation of a program of action.	Merriam-Webster

Term	Definition	Source
policy	A high-level, overall plan embracing the general goals and acceptable procedures of an organization.	Merriam-Webster
practice	An activity performed to support a domain goal.	CRR
resilience	See *operational resilience*.	
resilience requirement	A constraint that the organization places on the productive capability of an asset to ensure that it remains viable and sustainable when charged into production to support a service.	CRR
risk	Potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.	DHS Risk Lexicon 2010
risk disposition	A statement of the organization's intention for addressing operational risk. Typically limited to *accept*, *transfer*, *research*, or *mitigate*.	CERT-RMM

Risk Management (RM)	A domain of practice within the CRR. The purpose of risk management is to identify, analyze, and mitigate risks to critical service and IT assets that could adversely affect the operation and delivery of services.	CRR
risk tolerance	Thresholds that reflect the organization's level of risk aversion by providing levels of acceptable risk in each operational risk category that the organization has established.	Adapted from CERT-RMM
separation of duties	Separation of duties addresses the potential for abuse of authorized privileges by dividing roles and privileges between users.	NIST SP 800-53
service continuity/continuity of operations	An organization's ability to sustain assets and services in light of realized risk.	CERT-RMM
Service Continuity Management (SCM)	A domain of practice within the CRR. The purpose of service continuity management is to ensure the continuity of essential IT operations related to critical services and their associated assets if a disruption occurs as a result of an incident, disaster, or disruptive event.	CRR

Term	Definition	Source
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modeling and simulation) to support automated and/or human decision making (for example, concerning power system functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualization techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision making.	Adapted from SGMM Glossary
Situational Awareness (SA)	A domain of practice within the CRR. 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.	CRR
stakeholder	A person or organization that has a vested interest in the organization or its activities.	CERT-RMM

technology asset	Any hardware, software, or firmware used by the organization in the delivery of services.	CERT-RMM
threat	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 organization.	CERT-RMM
training	A set of activities that focuses on staff members learning the skills and knowledge needed to perform their roles and responsibilities in support of their organization's resilience program.	NIST SP 800-16
Training and Awareness (TA)	A domain of practice within the CRR. The purpose of training and awareness is to promote awareness and to develop skills and knowledge of people, in support of their roles in attaining, protecting, and sustaining critical services.	CRR

Term	Definition	Source
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.	DHS Risk Lexicon 2010
Vulnerability Management (VM)	A domain of practice within the CRR. The purpose of vulnerability management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.	CRR

APPENDIX C: REFERENCES

A Complete Guide to the Common Vulnerability Scoring System Version 2.0
http://www.first.org/cvss/v2/guide
Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
CERT® Resilience Management Model (CERT®-RMM)
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084
Cyber Hygiene: 11 Essential Practices
https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html
Special Publication 800-16 Revision 1 (DRAFT) "A Role-Based Model for Federal Information Technology/Cybersecurity Training (3rd Draft)"
https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/draft
FIPS Publication 199 "Standards for Security Categorization of Federal Information and Information Systems"
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems"
https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf
Framework for Improving Critical Infrastructure Cybersecurity
http://www.nist.gov/cyberframework/
Handbook for Computer Security Incident Response Teams (CSIRTs)
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
Managing for Enterprise Security
http://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
http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Special Publication 800-30 "Guide for Conducting Risk Assessments"
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Special Publication 800-34, "Contingency Planning for Federal Information Systems"
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Special Publication 800-37 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" 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"
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
Special Publication 800-40 Version 3.0 "Guide to Enterprise Patch Management Technologies"
http://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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Special Publication 800-61, "Computer Security Incident Handling Guide"
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Special Publication 800-70, “National Checklist Program for IT Products: Guidelines for Checklist Users and Developers”
https://csrc.nist.gov/publications/detail/sp/800-70/rev-4/final
Special Publication 800-84, “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities”
http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
Special Publication 800-128 "Guide for Security-Focused Configuration Management of Information Systems"
http://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”
http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

This page is intentionally blank.