DoD CYBER CRIME CENTER

DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

CYBER RESILIENCE ANALYSIS

Method Description and Self-Assessment User Guide

JUNE 2020

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

DM19-0303

CYBER RESILIENCE
ANALYSIS

Table of Contents

CYBER RESILIENCE
ANALYSIS

CYBER RESILIENCE
ANALYSIS

List of Figures

CYBER RESILIENCE
ANALYSIS

List of Tables

CYBER RESILIENCE
ANALYSIS

1 Introduction

1.1 Purpose of This Guide

The purpose of this document is to enable organizations to conduct a self-evaluation using the Cyber Resilience Analysis (CRA). The CRA Self-Evaluation provides a measure of an organization's cyber resilience capabilities. This user's guide

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

The CRA Self-Evaluation allows an organization to evaluate its capabilities relative to the requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations and the Cybersecurity Maturity Modle Certificaiton (CMMC). A crosswalk document that maps the CRA to NIST SP800-171 and CMMC are included as part of the CRA Self-Evaluation Kit. The use of the CRA is not intended to be a compliance activity. The CRA is a lightweight diagnostic tool an organization can utilize to quickly gain insights into its current NIST SP 800-171 and CMMC implementation posture and assist with its improvement efforts.

The CRA Self-Evaluation also enables an organization to evaluate its capabilities relative to v1.1 of the NIST Cybersecurity Framework (CSF), and a crosswalk document that maps the CRA to the NIST CSF is also included as a component of the CRA Self-Evaluation Kit. Though the CRA 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 CRA practices and capabilities may fall short of or exceed corresponding practices and capabilities in the NIST CSF.

The CRA reflects an organization's capabilities only at the time of the analysis. Even though certain aspects and questions in the CRA are designed to indicate the organization's ability to sustain cybersecurity practices over time, the organization should not rely on the analysis results as a conclusive expression of the organization's cybersecurity capability in the future.

[1] The CERT® Resilience Management Model (CERT®-RMM).

CYBER RESILIENCE
ANALYSIS

1.2 Intended Audience

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

1.3 How to Use This Guide

The facilitator should use this guide as a starting point for preparing and executing the CRA Self-Evaluation. Sections 3 through 5 of the guide correspond to the three key phases of a self-evaluation: CRA Self-Evaluation Form Completion, Report Interpretation, and Follow-Up. The facilitator should read through the entire guide and the supporting documents to become familiar with the CRA itself as well as the end-to-end process of executing the self-evaluation. Familiarity with the materials is important because each self-evaluation 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.

1.4 Organization of the Guide

Section 2, CRA Overview, describes the CRA architecture as well as the individual components that make up the CRA.

Sections 3 through 5 describe the three key phases of a typical self-evaluation process:

- Section 3: Conducting a CRA Self-Evaluation. The organization prepares for the self-evaluation, conducts the self-evaluation, and completes the form.
- Section 4: Interpreting the CRA Self-Evaluation Report. The results documented in the self-evaluation 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 provides a brief summary followed by the appendices, which contain a process checklist, a glossary of terms used in this document, and a list of references.

CYBER RESILIENCE
ANALYSIS

2 CRA Overview

2.1 CRA Method

The CRA is a lightweight analysis method that was created by the Department of Defense Cyber Crimes Center (DoD-DC3) for the purpose of evaluating the cybersecurity practices of partner organizations in the Defense Industrial Base Collaborative Information Sharing Program (DCISE). The CRA, consisting of 299 questions, is typically delivered in a six-hour workshop led by facilitators from DC3. The facilitators elicit answers from the critical infrastructure organization's personnel in cybersecurity, operations, physical security, and business continuity.

The CRA Self-Evaluation 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 CRA.

2.2 CRA Architecture

The CRA is an interview-based analysis 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 CRA focuses on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization. The CRA 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 CRA 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 CRA 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.

CYBER RESILIENCE
ANALYSIS

Table 1: CRA Domain Composition

CRA 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 CRA 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 CRA questions have three possible responses: "Yes," "No," and "Incomplete."

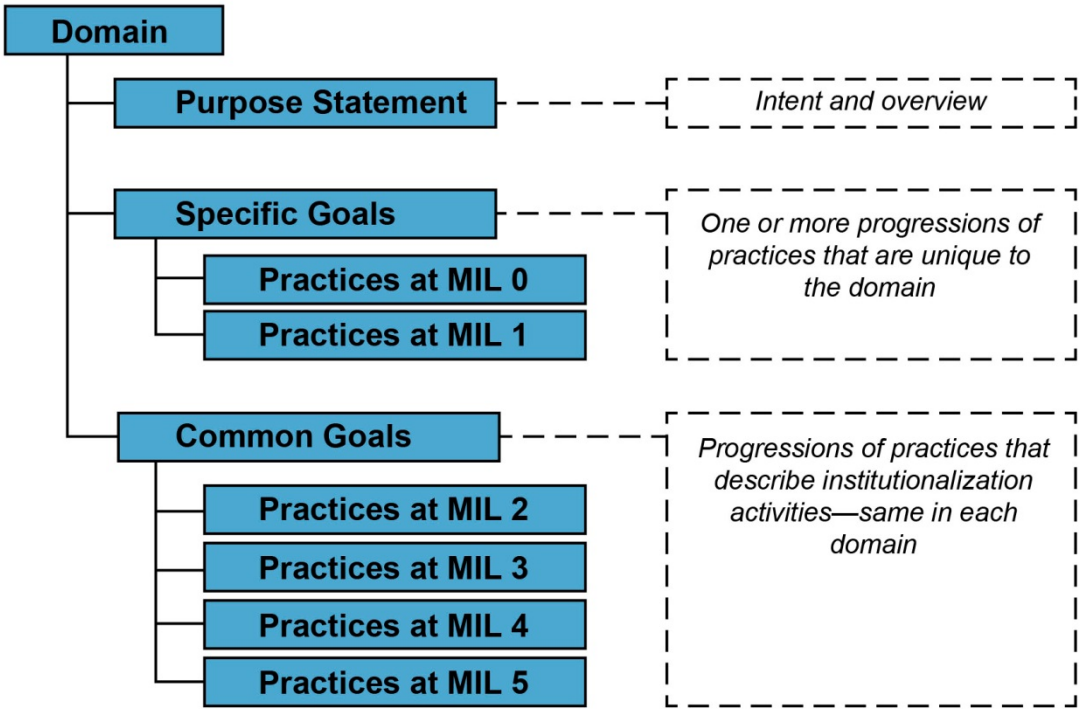

Figure 1: The Cyber Resilience Analysis Domain Architecture

CYBER RESILIENCE
ANALYSIS

2.3 Domain Descriptions

The following section describes the 10 CRA 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 CRA 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.**
    1. The organization's services are identified.
    2. The organization's services are prioritized based on analysis of the potential impact if the services are disrupted.
    3. The organization's mission, vision, values and purpose, including the organizations place in critical infrastructure, is identified and communicated.
    4. The organization's mission, objectives, and activities are prioritized.

2. **Assets are inventoried, and the authority and responsibility for these assets is established.**
    1. The assets that directly support the critical service are inventoried (technology includes hardware, software, and external information systems).
    2. Asset descriptions include protection and sustainment requirements.
    3. Owners and custodians of assets are documented in asset descriptions.
    4. The physical locations of assets (both within and outside the organization) are documented in the asset inventory.
    5. 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.**
    1. The associations between assets and the critical service they support are documented.
    2. Confidentiality, integrity, and availability requirements are established for each service-related asset.

4. **The asset inventory is managed.**
    1. Change criteria are established for asset descriptions.

2. Asset descriptions are updated when changes to assets occur.

5. **Access to assets is managed.**
    1. Access (including identities and credentials) to assets is granted based on their protection requirements.
    2. Access (including identities and credentials) requests are reviewed and approved by the asset owner.
    3. Access privileges are reviewed to identify excessive or inappropriate privileges.
    4. Access privileges are modified as a result of reviews.
    5. Access permissions are managed incorporating the principle of least privilege.
    6. Access permissions are managed incorporating the principle of separation of duties.
    7. 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.**
    1. Information assets are categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, or secret).
    2. The categorization of information assets is monitored and enforced.
    3. Policies and procedures for the proper labeling and handling of information assets are created.
    4. 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.
    5. High-value information assets are backed up and retained.
    6. Guidelines for properly disposing of information assets are created.
    7. Adherence to information asset disposal guidelines is monitored and enforced.

7. **Facility assets supporting the critical service are prioritized and managed.**
    1. 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.
    2. The prioritization of facilities is reviewed and validated.
    3. 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 CRA 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.**
    1. Control objectives are established for assets required for delivery of the critical service.
    2. Control objectives are prioritized according to their potential to affect the critical service.

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

3. **Control designs are analyzed to ensure they satisfy control objectives.**
    1. Control designs are analyzed to identify gaps where control objectives are not adequately satisfied.
    2. 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.**
    1. The performance of controls is assessed on a schedule to verify they continue to meet control objectives.
    2. As a result of scheduled assessments, new controls are introduced or existing controls are modified to address problem areas.

CYBER RESILIENCE
ANALYSIS

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

2. **The integrity of technology and information assets is managed.**
    1. Configuration management is performed for technology assets.
    2. Techniques are used to detect changes to technology assets.
    3. Modifications to technology assets are reviewed.
    4. Integrity requirements are used to determine which staff members are authorized to modify information assets.
    5. The integrity of information assets is monitored.
    6. Unauthorized or unexplained modifications to technology assets are addressed.
    7. Modifications to technology assets are tested before being committed to production systems.
    8. A process for managing access to technology assets is implemented.
    9. The maintenance and repair of assets is performed and logged in a timely manner.
    10. The maintenance and repair of assets is performed with approved and controlled tools and/or methods.
    11. 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.**
    1. Technology assets configuration baselines are created.
    2. Approval is obtained for proposed changes to baselines.
    3. A baseline of network operations is established.
    4. The baseline of network operations is managed.

5. A baseline of expected data flows for users and systems is established.
6. 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.**
    1. A vulnerability analysis and resolution strategy has been developed.
    2. There is a standard set of tools and/or methods in use to identify vulnerabilities in assets.
    3. A standard set of tools and/or methods is in use to detect malicious code in assets.
    4. A standard set of tools and/or methods is in use to detect unauthorized mobile code in assets.
    5. 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.**
    1. Sources of vulnerability information have been identified.
    2. The information from these sources is kept current.
    3. Vulnerabilities are being actively discovered.
    4. Vulnerabilities are categorized and prioritized.
    5. Vulnerabilities are analyzed to determine relevance to the organization.
    6. A repository is used for recording information about vulnerabilities and their resolution.
3. **Exposure to identified vulnerabilities is managed.**
    1. Actions are taken to manage exposure to identified vulnerabilities.
    2. The effectiveness of vulnerability mitigation is reviewed.
    3. The status of unresolved vulnerabilities is monitored.
4. **The root causes of vulnerabilities are addressed.**
    1. Underlying causes for vulnerabilities are identified (through root-cause analysis or other means) and addressed.

CYBER RESILIENCE
ANALYSIS

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.**
    1. The organization has a plan for managing incidents.
    2. The incident management plan is reviewed and updated.
    3. The roles and responsibilities in the plan are included in job descriptions.
    4. 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.**
    1. Events are detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information).
    2. Event data is logged in an incident knowledgebase or similar mechanism.
    3. Events are categorized.
    4. Events are analyzed to determine if they are related to other events.
    5. Events are prioritized.
    6. The status of events is tracked.
    7. Events are managed to resolution.
    8. Requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes are identified.
    9. A process to ensure event evidence is handled as required by law or other obligations is followed.

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

4. **A process for responding to and recovering from incidents is established.**
    1. Incidents are escalated to stakeholders for input and resolution.
    2. Responses to declared incidents are developed and implemented according to pre-defined procedures.

3. Incident status and response is communicated to affected parties (including public relations staff and external media outlets).
4. Incidents are tracked to resolution.

5. **Post-incident lessons learned are translated into improvement strategies.**
    1. Analysis is performed to determine the root causes of incidents.
    2. A link between the incident management process and other related processes (problem management, risk management, change management, etc.) is established.
    3. 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.**
    1. Service continuity plans are developed and documented for assets (people, information, technology, and facilities) required for delivery of the critical service.
    2. Service continuity plans are developed using established standards, guidelines, and templates.
    3. Staff members are assigned to execute specific service continuity plans.
    4. Key contacts are identified in the service continuity plans.
    5. Service continuity plans are stored in a controlled manner and available to all those who need to know.
    6. Availability requirements such as recovery time objectives and recovery point objectives are established.
    7. 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.**
    1. Plans are reviewed to identify and resolve conflicts.

3. **Service continuity plans are tested to ensure they meet their stated objectives.**
    1. Standards for testing service continuity plans have been implemented.
    2. A schedule for testing service continuity plans has been established.
    3. Service continuity plans are tested.

4. Backup and storage procedures for high-value information assets are tested.
5. Test results are compared with test objectives to identify needed improvements to service continuity plans.

4. **Service continuity plans are executed and reviewed.**
    1. Conditions have been identified that trigger the execution of the service continuity plan.
    2. The execution of service continuity plans is reviewed.
    3. 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 CRA focuses on risks to cyber-dependent operations that have the potential to interrupt delivery of the critical service being examined. While the CRA 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.**
    1. Sources of risk that can affect operations have been identified.
    2. Categories for risks have been established.
    3. A plan for managing operational risk has been established.
    4. 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.**
    1. Impact areas, such as reputation, financial health, and regulatory compliance, have been identified.
    2. Impact areas have been prioritized to determine their relative importance.
    3. Risk tolerance parameters have been established for each impact area.
    4. Risk tolerance thresholds, which trigger action, are defined for each category of risk.

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

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

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

CYBER RESILIENCE
ANALYSIS

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 CRA 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.**
    1. Dependencies on external relationships that are critical to the service are identified.
    2. A process has been established for creating and maintaining a list of external dependencies.
    3. External dependencies are prioritized.

2. **Risks due to external dependencies are identified and managed.**
    1. Risks due to external dependencies are identified and managed.

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

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

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

CYBER RESILIENCE
ANALYSIS

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 focuses 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.**
    1. Cybersecurity awareness needs have been identified for the critical service.
    2. Required skills have been identified for specific roles (administrators, technicians, etc.) for the critical service.
    3. Skill gaps present in personnel responsible for cybersecurity are identified.
    4. Training needs have been identified.

2. **Awareness and training activities are conducted.**
    1. Cybersecurity awareness activities for the critical service are conducted.
    2. Cybersecurity training activities for the critical service are conducted.
    3. The effectiveness of the awareness and training programs is evaluated.
    4. Awareness and training activities are revised as needed.
    5. Privileged users are trained in their specific roles and responsibilities in support of the critical service.
    6. Senior executives are trained in their specific roles and responsibilities in support of the critical service.
    7. 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.

CYBER RESILIENCE
ANALYSIS

The Situational Awareness domain comprises three goals and eight practices:

1. **Threat monitoring is performed.**
    1. Responsibility for monitoring sources of threat information has been assigned.
    2. Threat monitoring procedures have been implemented.
    3. Resources have been assigned and trained to perform threat monitoring.
2. **The requirements for communicating threat information are established.**
    1. Internal stakeholders (such as the critical service owner and incident management staff) to whom threat information must be communicated have been identified.
    2. 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.**
    1. Threat information is communicated to stakeholders.
    2. Resources have been assigned authority and accountability for communicating threat information.
    3. Resources have been trained with respect to their specific role in communicating threat information.

2.4 MIL Scale

The CRA uses Maturity Indicator Levels (MILs) to provide organizations with an approximation of the maturity of their practices in the 10 cybersecurity domains. The CRA's approach to maturity is based on an underlying capability maturity model, the CERT Resilience Management Model.[2] In this approach, the organization's maturity is based on how completely the cybersecurity practices in each of the domains are institutionalized within the organization.

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.

[2] In its simplest form, a *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. The artifacts that make up the model are typically agreed on by the domain or discipline, which validates them through application and refinement.

CYBER RESILIENCE
ANALYSIS

The following example illustrates how MILs may be applied to the CRA 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 CRA.*
>
> *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 CRA'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 CRA 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 CRA questions.

CYBER RESILIENCE
ANALYSIS

MIL2 Planned
All specific practices in the CRA 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.

CYBER RESILIENCE
ANALYSIS

3 Conducting a CRA Self-evaluation

3.1 Organizing for the Self-Evaluation

Identifying the Scope of the Self-Evaluation

It is expected that the facilitator will help the sponsor and the organization identify the scope of the self-evaluation. This scoping exercise is critical because answers to the self-evaluation questions must be provided in relation to a specific service. The scope of the self-evaluation is determined by three factors:

1. Critical service scope

   Ask: Which service will be the focus of the self-evaluation?

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

The CRA uses an identified critical service to frame the questions in the CRA. Therefore you must select a critical service in your organization that will serve as the focus of the analysis. 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 CRA strives to identify how an organization aligns its cybersecurity management activities to the performance or production of its critical services. Often, an organization's product suite provides a useful starting point for identifying a service. The following questions can help users identify their organization's critical services:

Which services 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)?

CYBER RESILIENCE
ANALYSIS

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 CRA:

- 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 CRA Self-Evaluation

The CRA Self-Evaluation is conducted in a group setting with a facilitator leading a group discussion. During the course of the self-evaluation, 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 CRA domains. The consensus answer is then recorded in the self-evaluation form before moving on to the next question.

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

Key Roles in the Self-Evaluation Process

A successful CRA Self-Evaluation 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 self-evaluation.

Table 2: Key Roles in the Self-Evaluation Process

Role	Description and Responsibilities
sponsor	The sponsor should have a broad understanding of the importance and components of the service for which the self-evaluation is being completed. General responsibilities include • deciding whether the organization should conduct a CRA Self-Evaluation • selecting an individual to serve as the facilitator • ensuring that the resources necessary for the self-evaluation are available • communicating the organization's support for the self-evaluation
facilitator	The facilitator is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the CRA Self-Evaluation. General responsibilities include • completing the three phases of a self-evaluation process • working with the organization to ensure the self-evaluation produces high-quality results • facilitating the completion of the self-evaluation form • generating the CRA Self-Evaluation report • distributing the CRA Self-evaluation report to the sponsor and designees • assisting in the planning of follow-on activities
subject matter experts (SMEs)	During the self-evaluation, 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 evaluated • able to represent one or more of the organization's activities in the CRA's 10 domains

Meeting with the Sponsor and Other Stakeholders

Prior to setting a date for the planned self-evaluation, the facilitator should meet with the sponsor and other stakeholders identified by the sponsor to prepare the organization for the self-evaluation.

The objectives of this meeting include the following:

- Familiarize the sponsor and/or stakeholders with the CRA.
- Obtain executive support for the self-evaluation.
- Shape the stakeholders' expectations for the self-evaluation (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 CRA Self-Evaluation 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 CRA. There should be SMEs familiar with how the organization operates in all 10 CRA 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 self-evaluation (e.g., scribes, IT support).

Preparing for the Workshop

Together with the sponsor and support staff, the facilitator schedules the workshop. A self-evaluation 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 self-evaluation 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 CRA Self-Evaluation 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 CRA Self-Evaluation 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 CRA. The facilitator should ensure that the workshop participants are prepared and comfortable during the workshop.

CYBER RESILIENCE
ANALYSIS

Table 4 describes several topics that previous CRA analysis 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 CRA 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 self-evaluation 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 self-evaluation, 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 self-evaluation 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 self-evaluation questions. Remember that open dialog and consensus building is as important as the completed self-evaluation.

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 analysis progresses, it is helpful to display the questions and the responses participants have already provided. The facilitator controls the responses recorded on the self-evaluation 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 self-evaluation questions but rather helps the group come to a consensus response. By facilitating the workshop, the

CYBER RESILIENCE
ANALYSIS

facilitator helps the organization answer the self-evaluation 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 CRA question guidance is useful in coming to this understanding.

3.2 Completing the Self-Evaluation

The CRA Self-Evaluation Package is contained within a single Adobe PDF file. The self-evaluation provides the following:

- CRA question set with guidance
- Collection method for answers
- Automated scoring
- A report with the detailed results and suggested options for consideration

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

System Requirements and Setup

The package must be completed using the latest version of Adobe Reader or Adobe Acrobat on both the Windows and Mac operating systems. Using other, third-party PDF applications may result in erratic behavior or and often results in corruption of the results.

Using the Self-Evaluation

The package enables simple collection of analysis data by using text fields, dropdown boxes, and checkboxes. It begins with basic profile information about the facilitator and organization (Figure 2). To enter data, click in any field and type the appropriate information. Use the Tab key or click in another field to move forward.

CYBER RESILIENCE
ANALYSIS

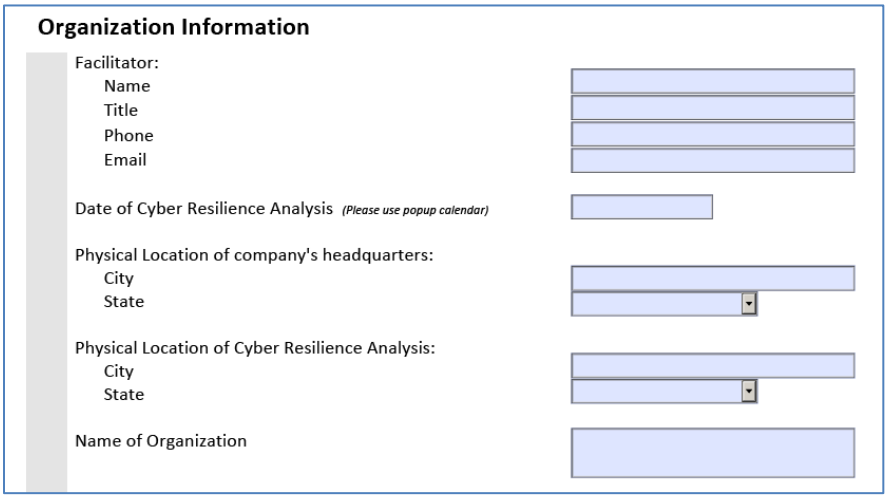

Figure 2: Profile Information

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

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

The CRA divides assets into four categories: People, Information, Technology, and Facilities. Some questions require a separate answer for each of the four assets while other questions refer to all assets. Figure 3 shows the two types of questions.

CYBER RESILIENCE
ANALYSIS

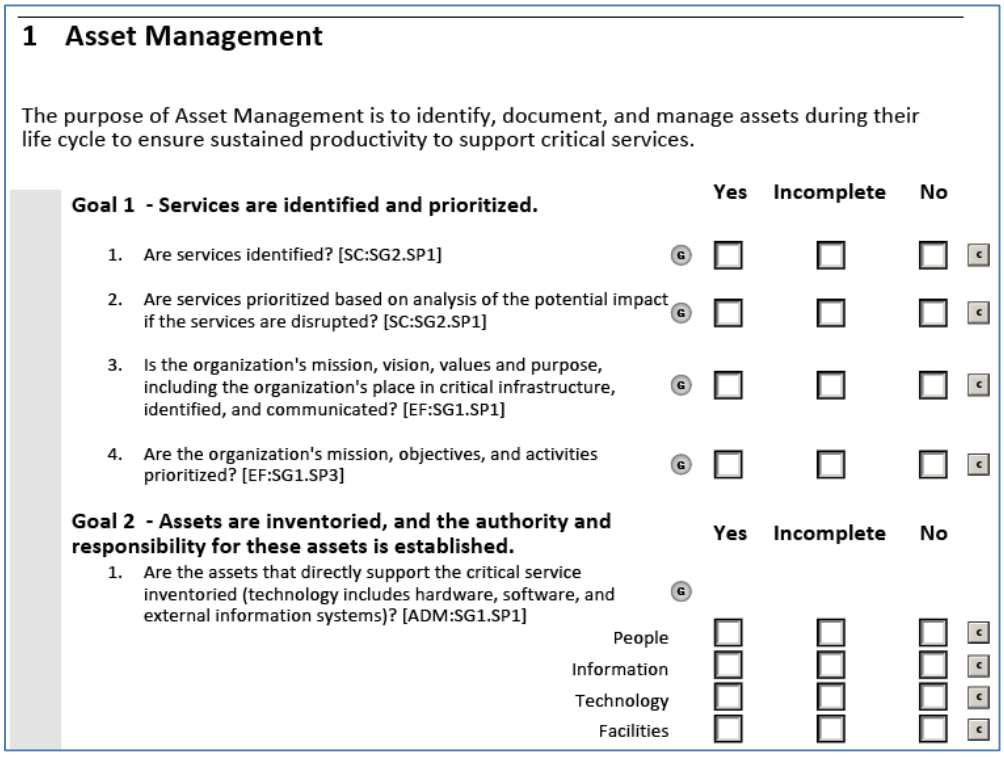

Figure 3: Cross-Asset Question and Per-Asset Question

Guidance

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

To aid the facilitator, each question is supported by guidance. Clicking on the [G] icon opens pop-up information that explains the question and answers (Figure 4).

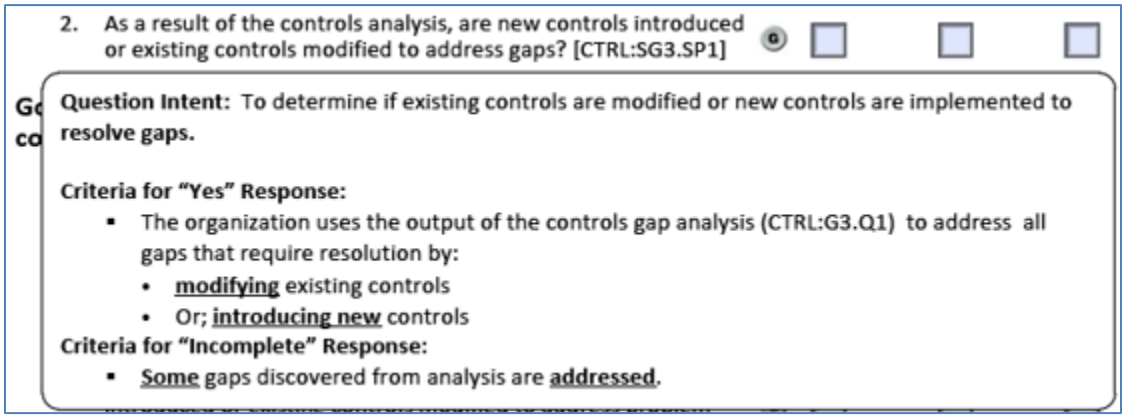

Figure 4: Explanatory Information

CYBER RESILIENCE
ANALYSIS

Additional Guidance for CMMC

In order to provide a more accurate representation of an organization's CMMC implementation posture, additional guidance was created to aid the facilitators with some of the questions in the CRA.

The GG icon represents a question that has additional guidance that further details CMMC requirements. By clicking on the second button the tool opens pop-up information that includes a table of the exact CMMC practices that are mapped to the specified CRA question as well as the criteria for a "yes" or "incomplete" response. For example, the additional guidance for Controls Management Goal 2 Question 1 produces a CMMC practice table that allows a facilitator to select each control that has already implemented to better track the current posture of the organization (Figure 5). The selections for the controls in the data capture form also translate to the generated report.

Organizations in the Defense Industrial Base should be cognizant of the practices contained within Cybersecurity Maturity Model Certification (CMMC). The CMMC practices that should be considered when evaluating this CRA practice include:

CMMC Practices

AC.2.009 Limit unsuccessful logon attempts. ☐	AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity. ☒	AC.3.019 Terminate (automatically) a user session after a defined condition. ☐
IA.3.083 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. ☒	IA.3.084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. ☒	IA.3.085 Prevent reuse of identifiers for a defined period. ☐
IA.3.086 Disable identifiers after a defined period of inactivity. ☒	IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created. ☒	IA.2.079 Prohibit password reuse for a specified number of generations. ☐
IA.2.080 Allow temporary password use for system logons with an immediate change to a permanent password. ☒	IA.2.081 Store and transmit only cryptographically-protected passwords ☒	IA.2.082 Obscure feedback of authentication information. ☐
PE.1.134 Control and manage physical access devices. ☒	SC.3.186 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. ☒	

The Navigator should use the table above to select the CMMC practice that the organization implements. This information will allow the organization to accurately track the CMMC practices they have in place to focus on practices that are not implemented.

Criteria for "Yes" Response:

- The organization has **implemented controls** to satisfy **all** the established control objectives.
- **All of the CMMC practices** listed in the guidance for this practice are **implemented, addressed, or considered in the context of the practice.**

Criteria for "Incomplete" Response:

- Controls have been implemented for **some** control objectives.
- Or; controls have been implemented **without** the establishment of control objectives.

Figure 5: Additional CMMC Guidance

CYBER RESILIENCE
ANALYSIS

Observations

At the end of each domain is a box labeled “Other Observations” (Figure 6). Any text entered in this box is copied verbatim into the report. It can be used to capture information such as reasoning or organization-specific information.

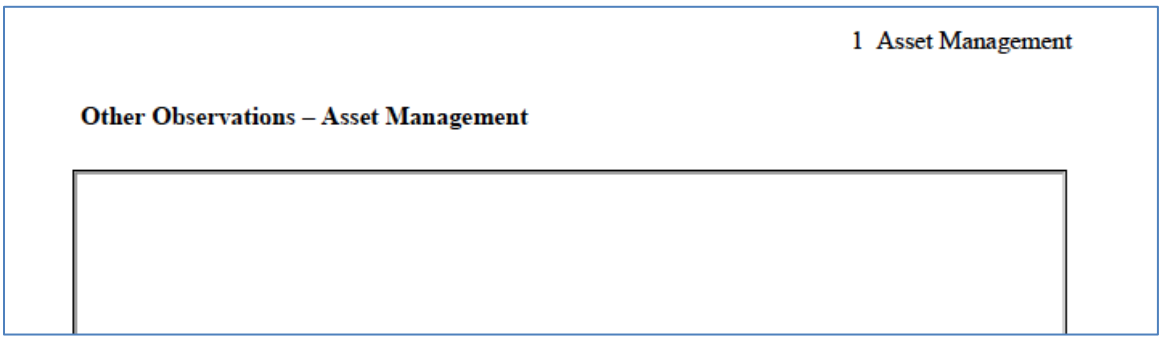

Figure 6: Entry Field for Other Observations

You should frequently save the document to prevent potential data loss.

Generating the Report

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

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

CYBER RESILIENCE
ANALYSIS

4 Interpreting the CRA Self-Evaluation Report

4.1 CRA 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

CYBER RESILIENCE
ANALYSIS

- 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 analysis-based instrument.

4.2 How to Interpret the Report

Scores

The organization may use the CRA Self-Evaluation Report to create an action plan for addressing weaknesses and leveraging strengths identified in the self-evaluation. A good place to start is with the CRA Performance Summary; Figure 7 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 7, the color-coded map of results by domain, combined with the individual domain results as shown in Figure 9, is useful for identifying areas for improvement.

CYBER RESILIENCE
ANALYSIS

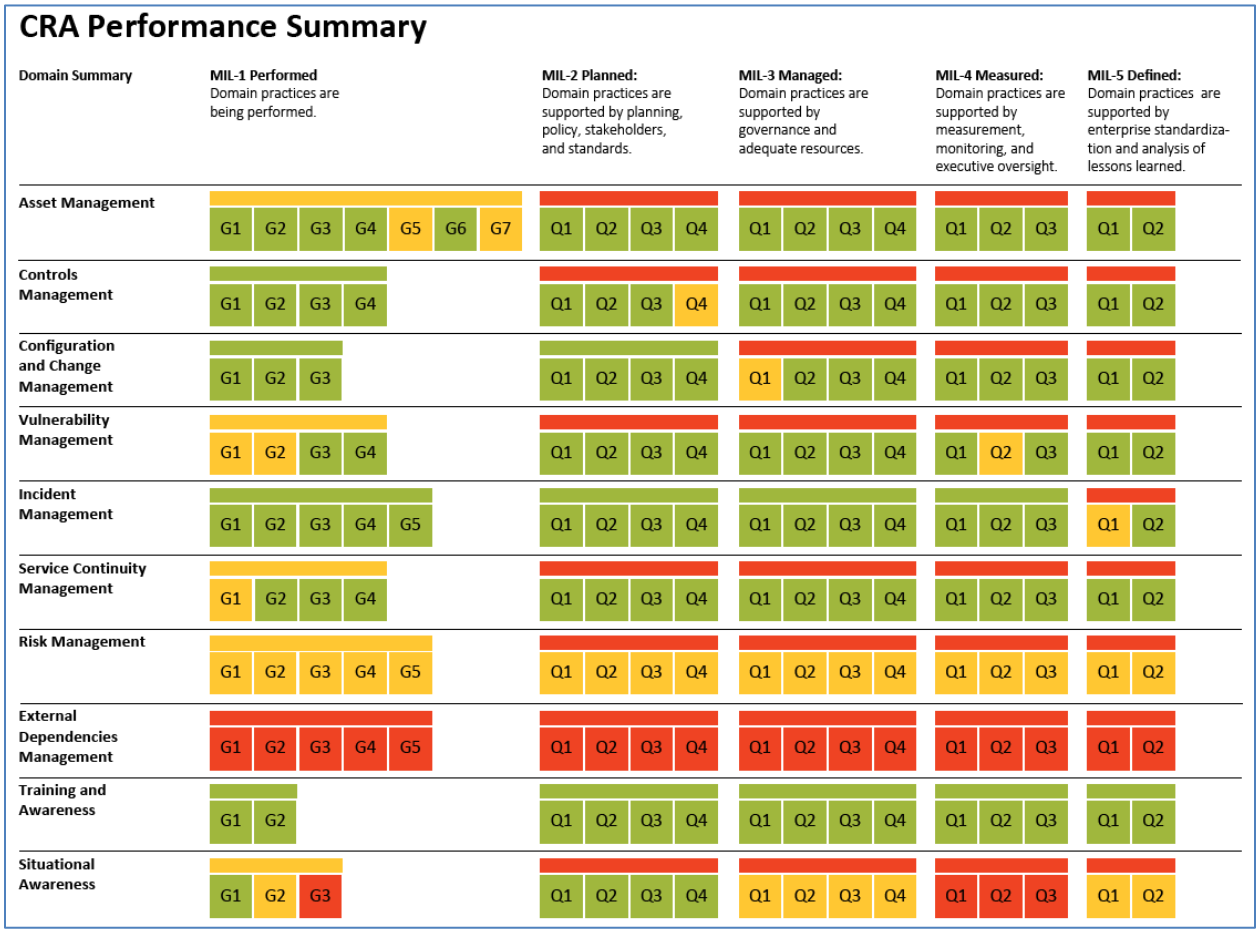

Figure 7: CRA Performance Summary

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.

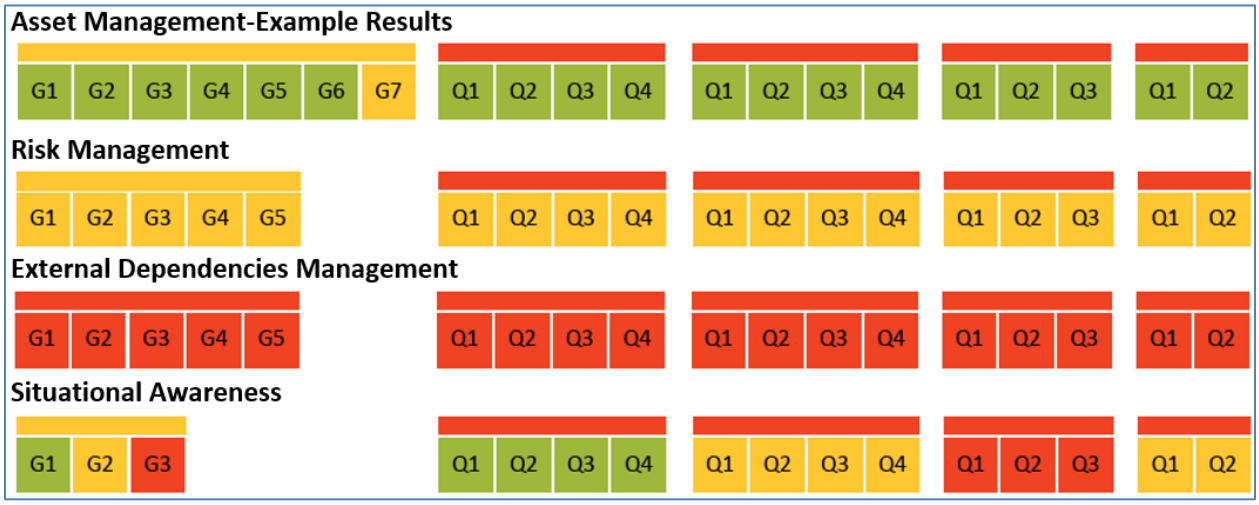

Figure 8: A Sampling of Individual Domains

Figure 8 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 9 and Figure 10, provide question-level detail to help organizations focus on specific practices for improvement.

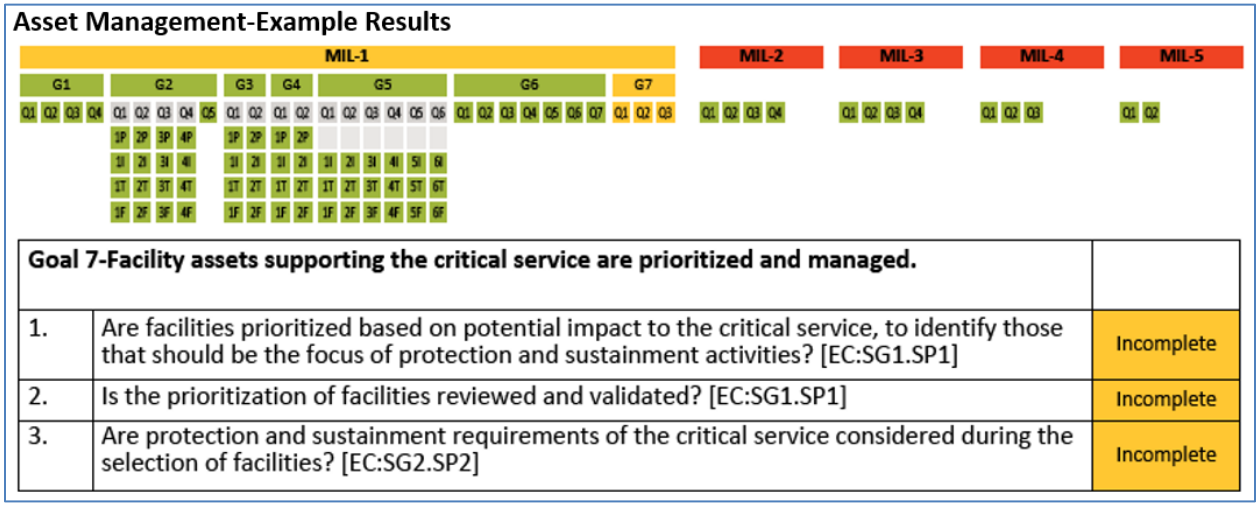

Figure 9: Asset Management Individual Domain Report

CYBER RESILIENCE
ANALYSIS

In the Asset Management scenario shown in Figure 9, 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.

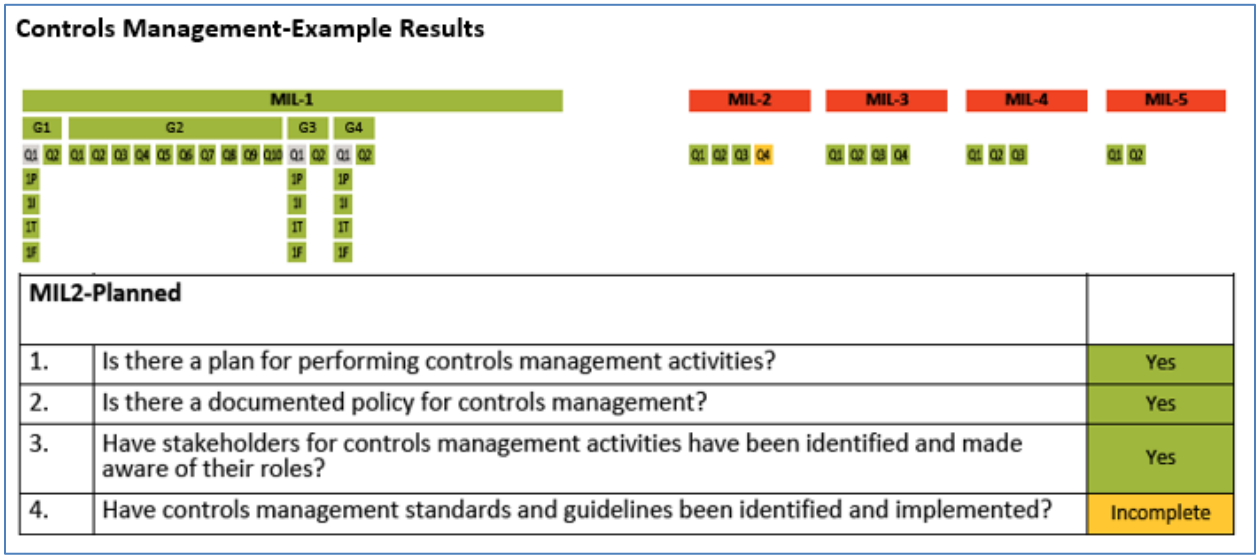

Figure 10: Controls Management Individual Domain Report

In the Controls Management scenario shown in Figure 10, 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.

CYBER RESILIENCE
ANALYSIS

The CRA MIL1 Performance Summary shown in Figure 11 provides an in depth summary of MIL1 goals and practices for each CRA 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 CRA.

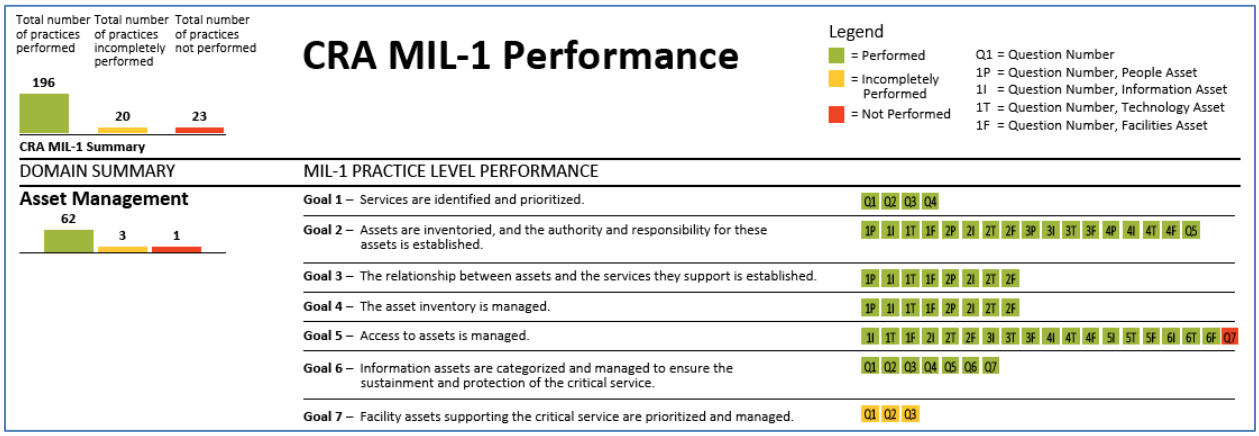

Figure 11: CRA MIL-1 Performance Summary – Asset Management

Similarly, The CRA MIL1 Performance depiction shown in Figure 12 provides a finer level of operational detail. In the Vulnerability Management scenario presented in Figure 12 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.

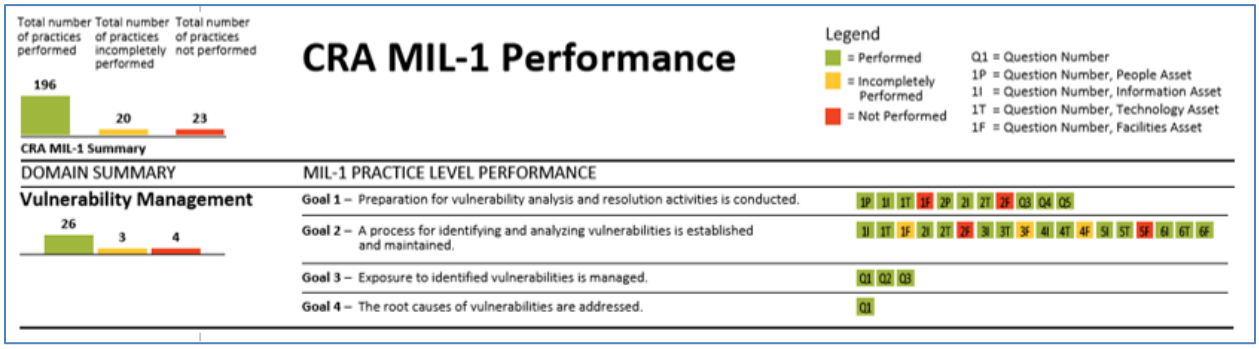

Figure 12: CRA MIL-1 Performance – Vulnerability Management

Additionally, the CRA Performance depiction shown in Figure 13 and located in Appendix A of the report provides a detailed operational view of the entire CRA.

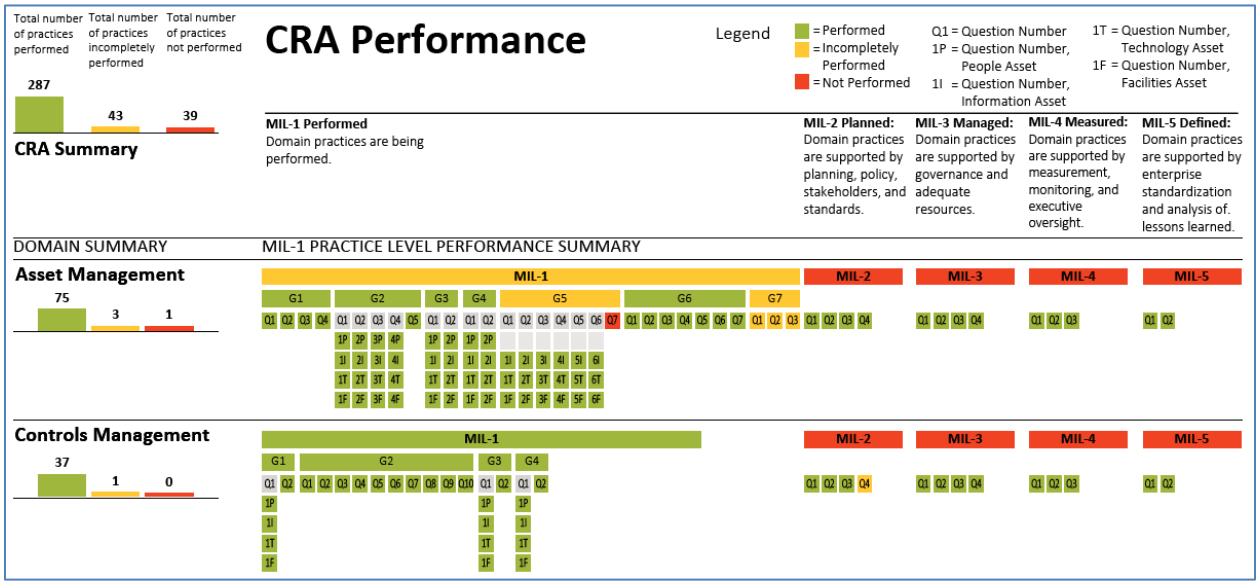

Figure 13: CRA Performance View

Figure 14 and Figure 15 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 14 shows that MIL1 was not achieved for the Asset Management domain, Figure 15 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.

CYBER RESILIENCE
ANALYSIS

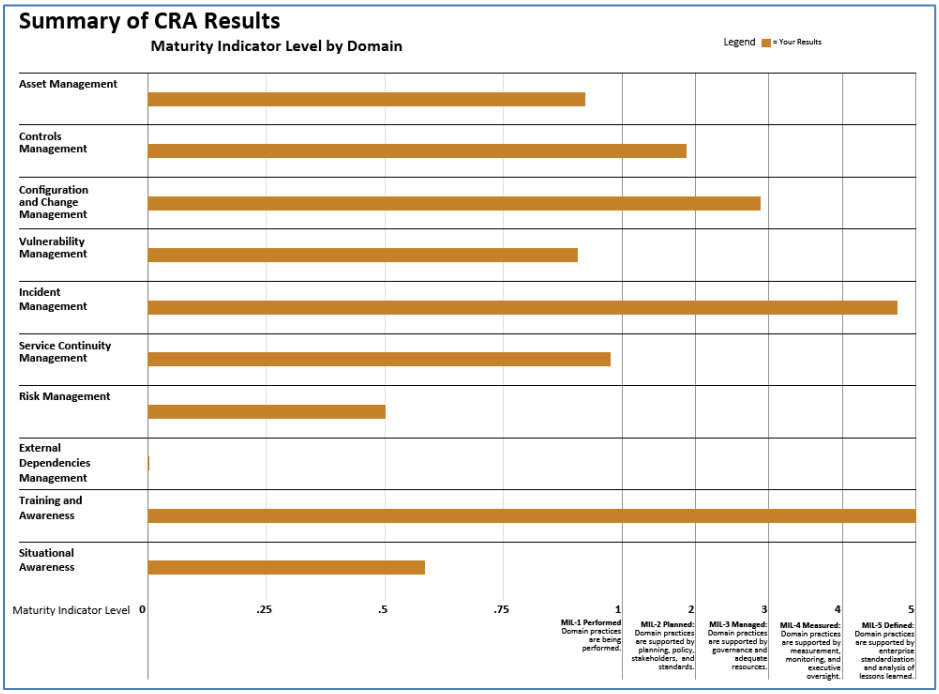

Figure 14: Summary of CRA Results

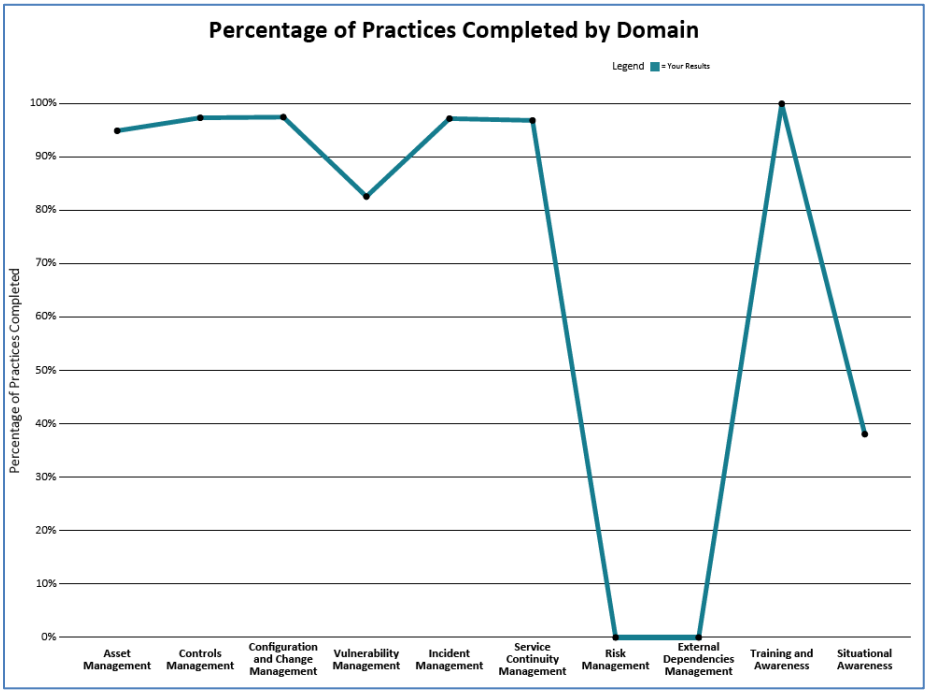

Figure 15: Percentage of Practices Completed by Domain

CYBER RESILIENCE
ANALYSIS

CMMC Scoring Depictions

The CRA Self-Evaluation also enables an organization to evaluate its capabilities relative to the requirements in the Cybersecurity Maturity Model Certification. Each CRA practice has been mapped to the applicable domains in CMMC. Figure 16 displays the organization's results by the 17 CMMC domains. An organization can use the requirements overview depiction to focus on prioritizing the CMMC domains it chooses to improve. For example, while the organization is performing 79% of the practices that comprise the Configuration Management domain, the results also show that the organization is only performing about 24% of the practices associated with the Risk Management domain. Therefore, the organization may choose to prioritize the implementation of practices that would lead to the improvement of the Risk Management Domain as it is currently an area of greater risk.

CYBER RESILIENCE
ANALYSIS

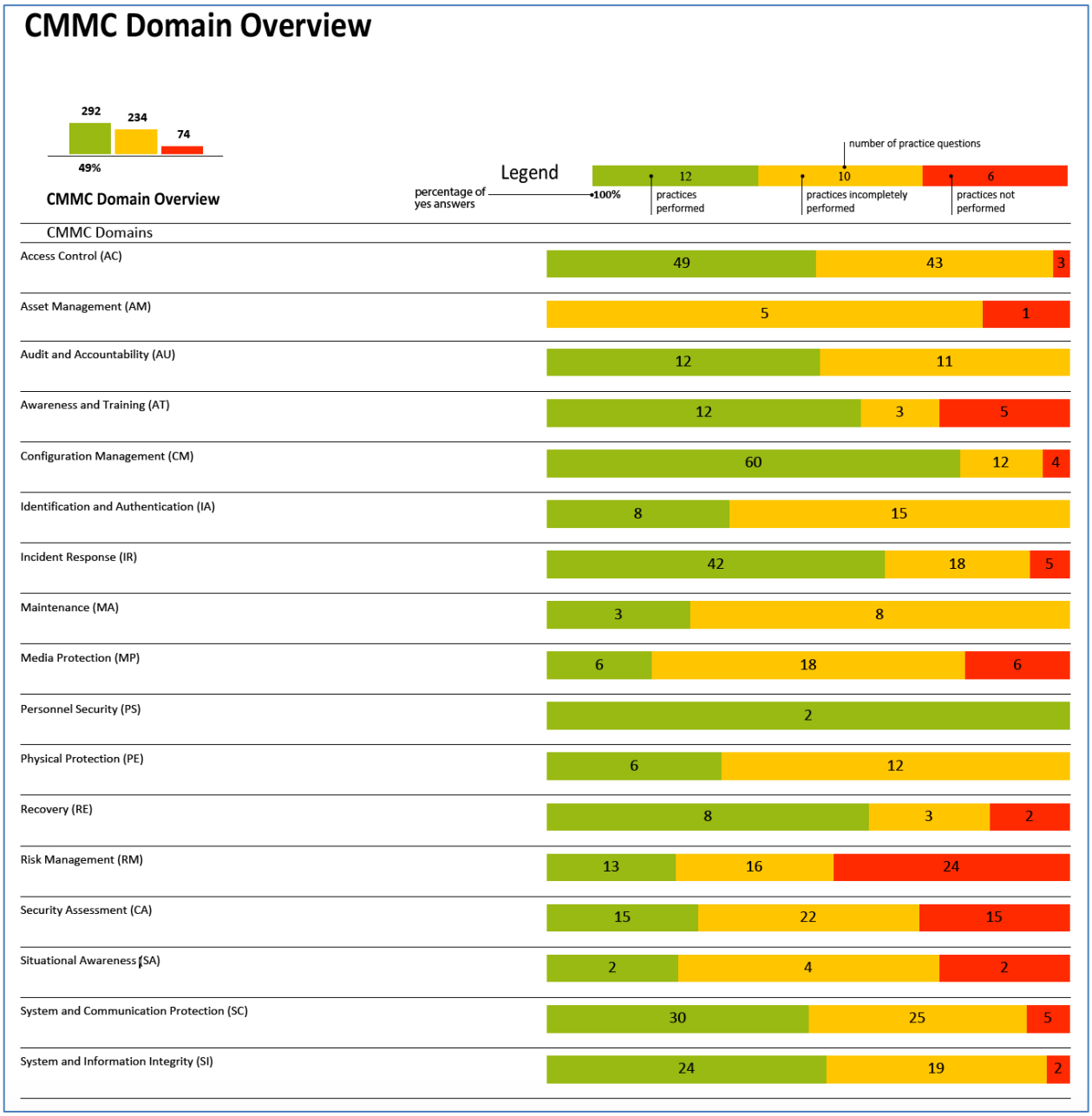

Figure 16: CMMC Domain Overview

NIST SP800-171 Scoring Depictions

The CRA Self-Evaluation also enables an organization to evaluate its capabilities relative to the requirements in NIST SP800-171 “Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations”. Each CRA practice has been mapped to the applicable security requirement families in NIST SP800-171. Figure 17 displays the organization’s results by the 14 security requirement families. An organization can use the requirements overview depiction to focus on prioritizing the security requirement families it chooses to improve. For example, while the organization is performing

CYBER RESILIENCE ANALYSIS

70% of the practices that comprise the Awareness and Training family, the results also show that the organization is only performing about 9% of the practices associated with the Access Control family. Therefore, the organization may choose to prioritize the implementation of practices that would lead to the improvement of the Access Control Family as it is currently an area of greater risk.

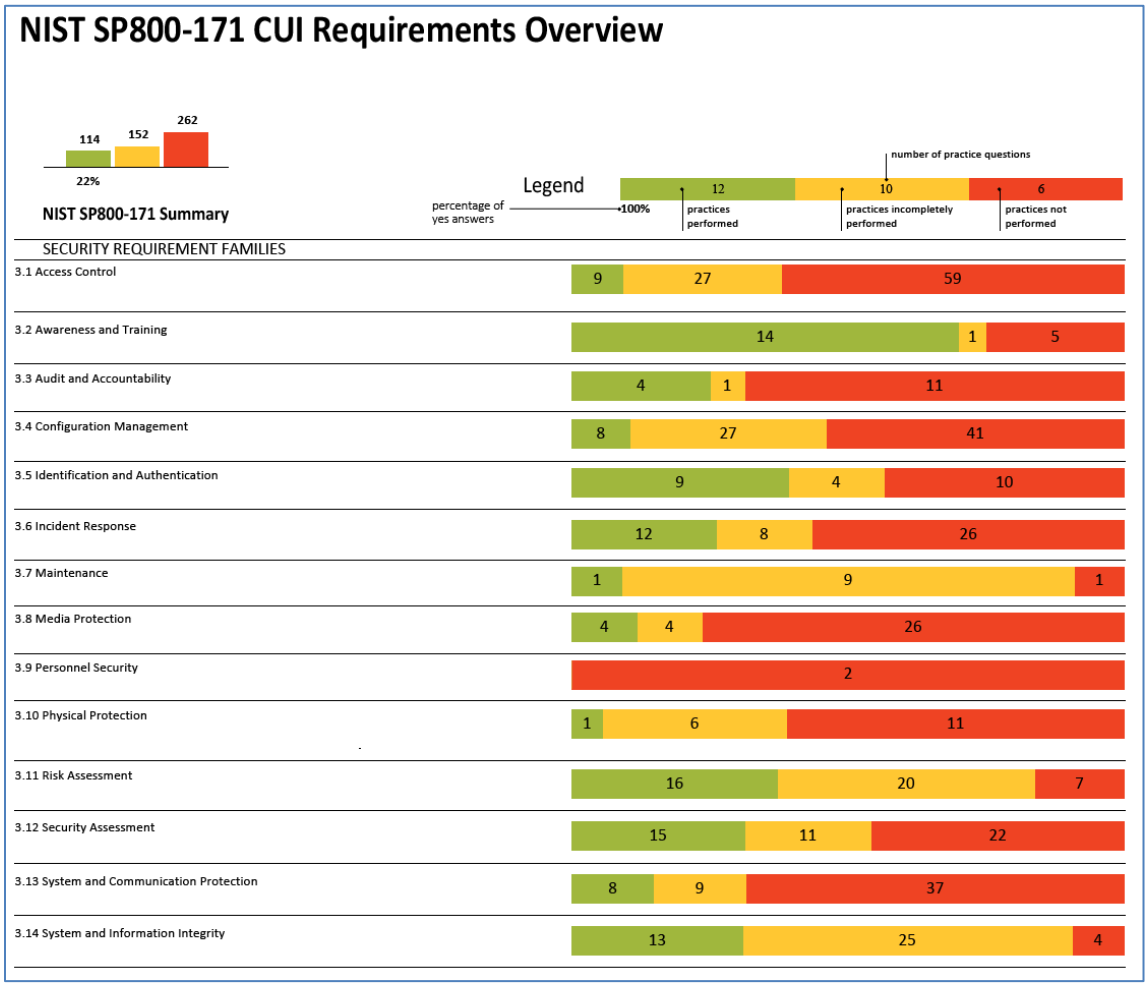

Figure 17: NIST SP800-171 CUI Requirements Overview

The CRA also contains other NIST SP800-171 depictions located in Appendix A. These depictions show a more detailed view of the security requirement families. Figure 18 depicts the performance of the Access Control security requirement family based on the organization's CRA responses. The depiction shows each Access Control requirement and the number of CRA practices that inform this requirement. For instance, requirement 3.1.1 has 12 unique CRA practices mapped to it. By performing each of the 12 questions an organization would be well on its way to having a framework in place that would satisfy this requirement. The example below highlights that the organization is incompletely performing 4 of the practices and not performing the other 8 practices. This quickly shows the organization is struggling to limit access to its important assets.

CYBER RESILIENCE
ANALYSIS

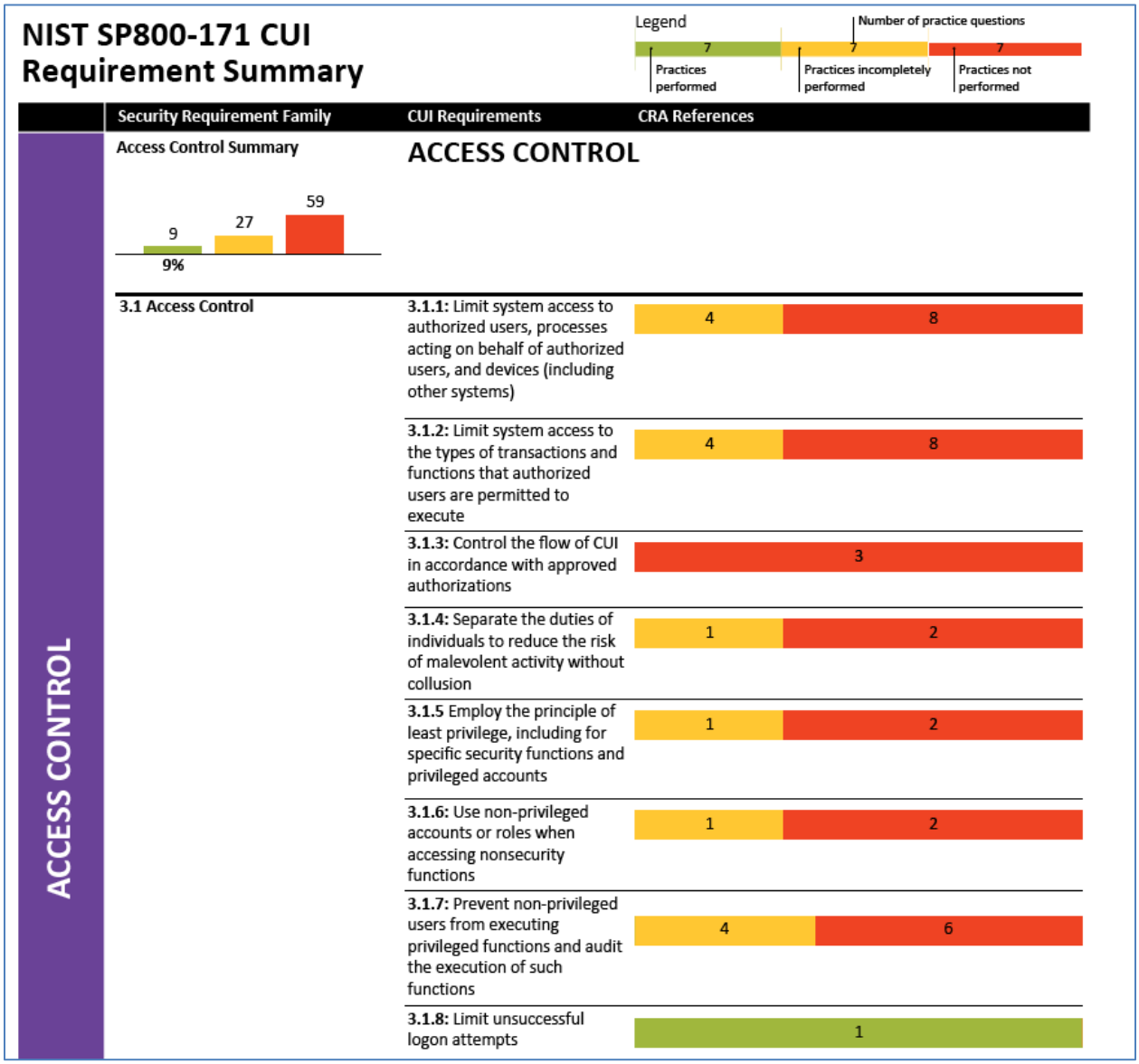

Figure 18: NIST SP800-171 CUI Requirement Summary

An organization can also use the NIST SP800-171 CUI Requirement Performance depiction (Figure 19) to view the organization's coverage of the security requirement families and to track its improvement efforts. The depiction acts a dynamic crosswalk for the user, and can quickly be referenced to see which CRA practices are mapped to specific CUI requirements.

CYBER RESILIENCE
ANALYSIS

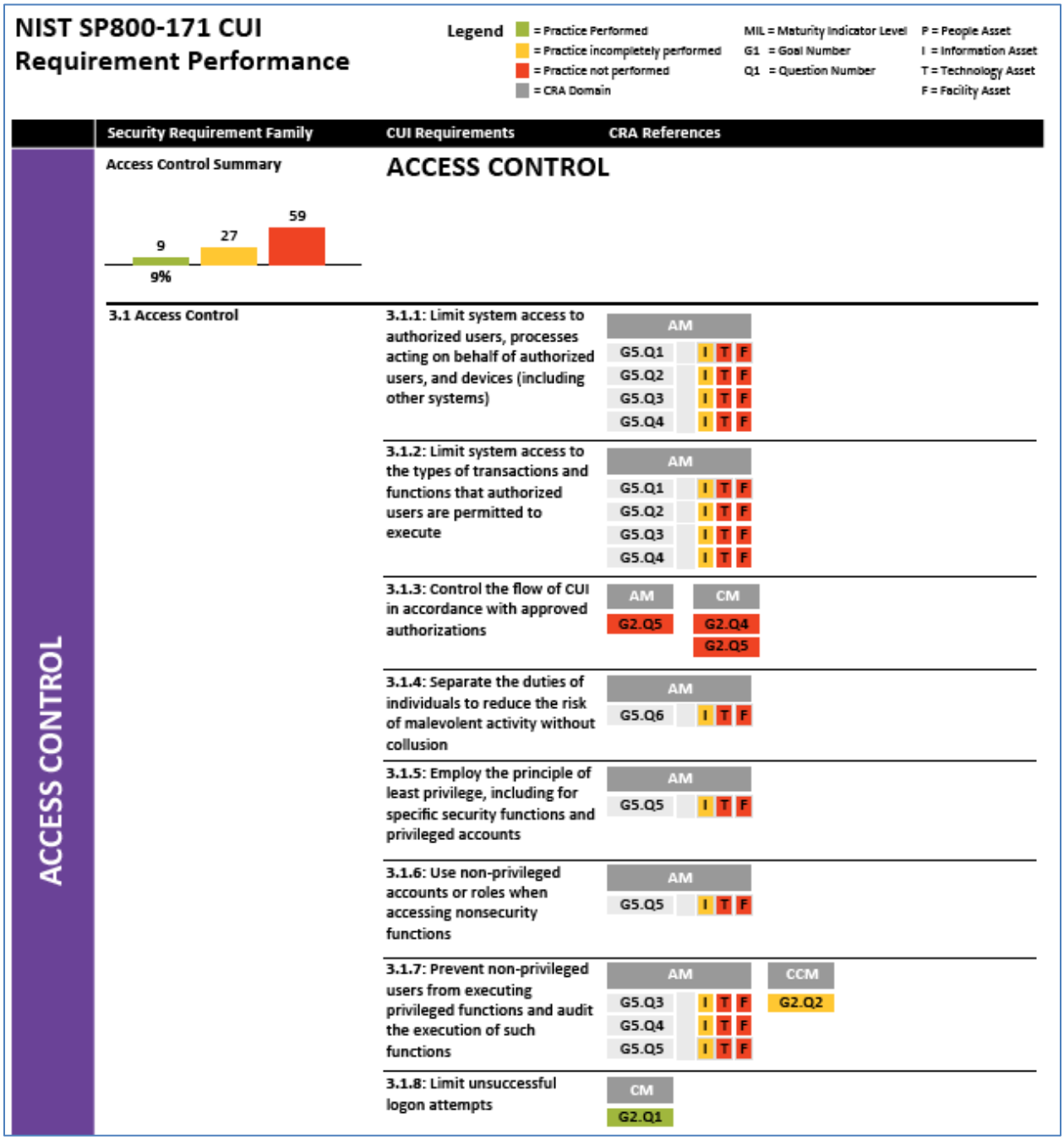

Figure 19: NIST SP800-171 CUI Requirement Performance

NIST Cybersecurity Framework Scoring Depictions

The CRA Self-Evaluation also enables an organization to evaluate its capabilities relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Each CRA practice has been mapped to the applicable categories and subcategories of the NIST CSF. Figure 20: NIST Cybersecurity Framework Summary displays the organization's results by function and category. An organization can

CYBER RESILIENCE
ANALYSIS

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.

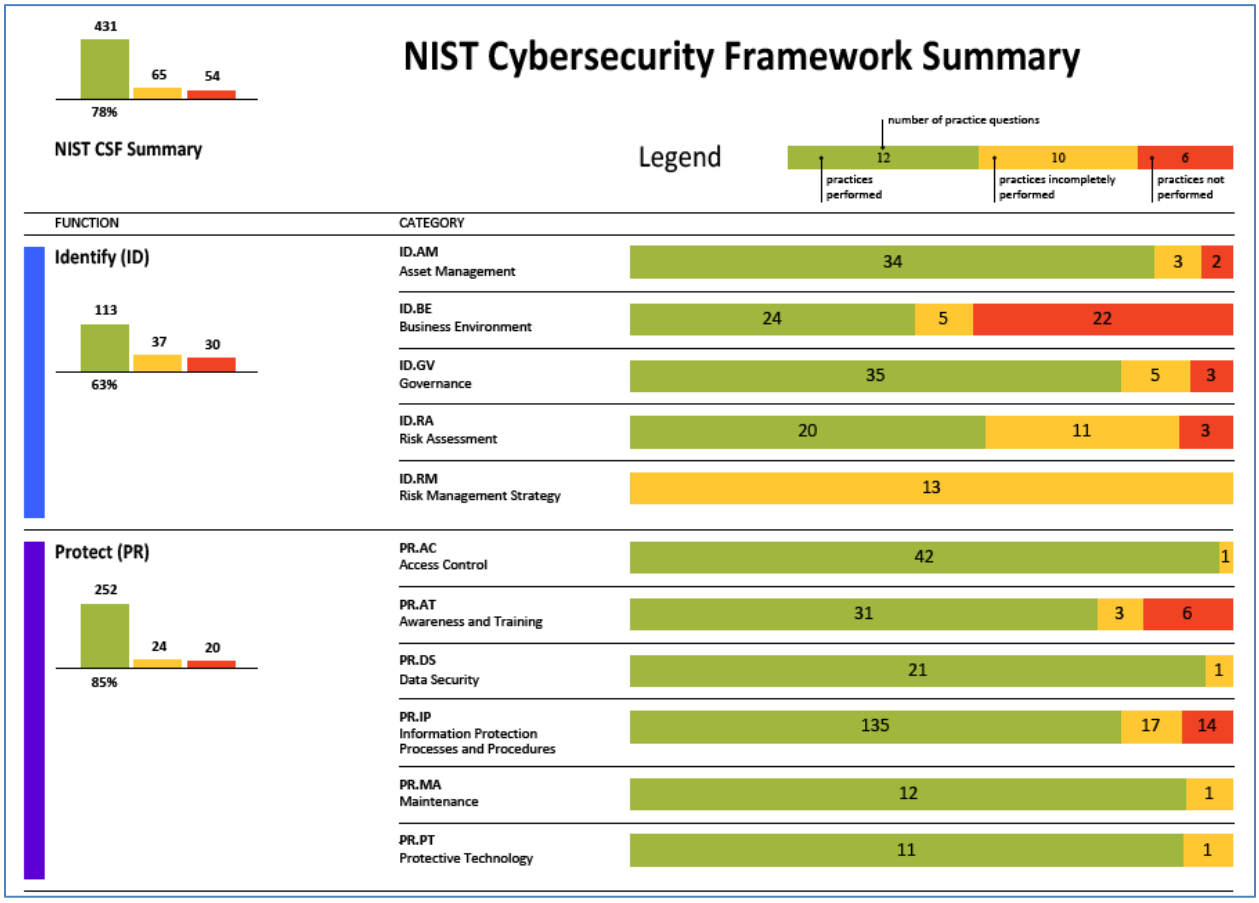

Figure 20: NIST Cybersecurity Framework Summary

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 21 depicts the performance of the Identify Function Asset Management Category based on the organization's CRA responses. It is important to note that the ID.AM Category has 19 unique CRA 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 CRA 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

CYBER RESILIENCE
ANALYSIS

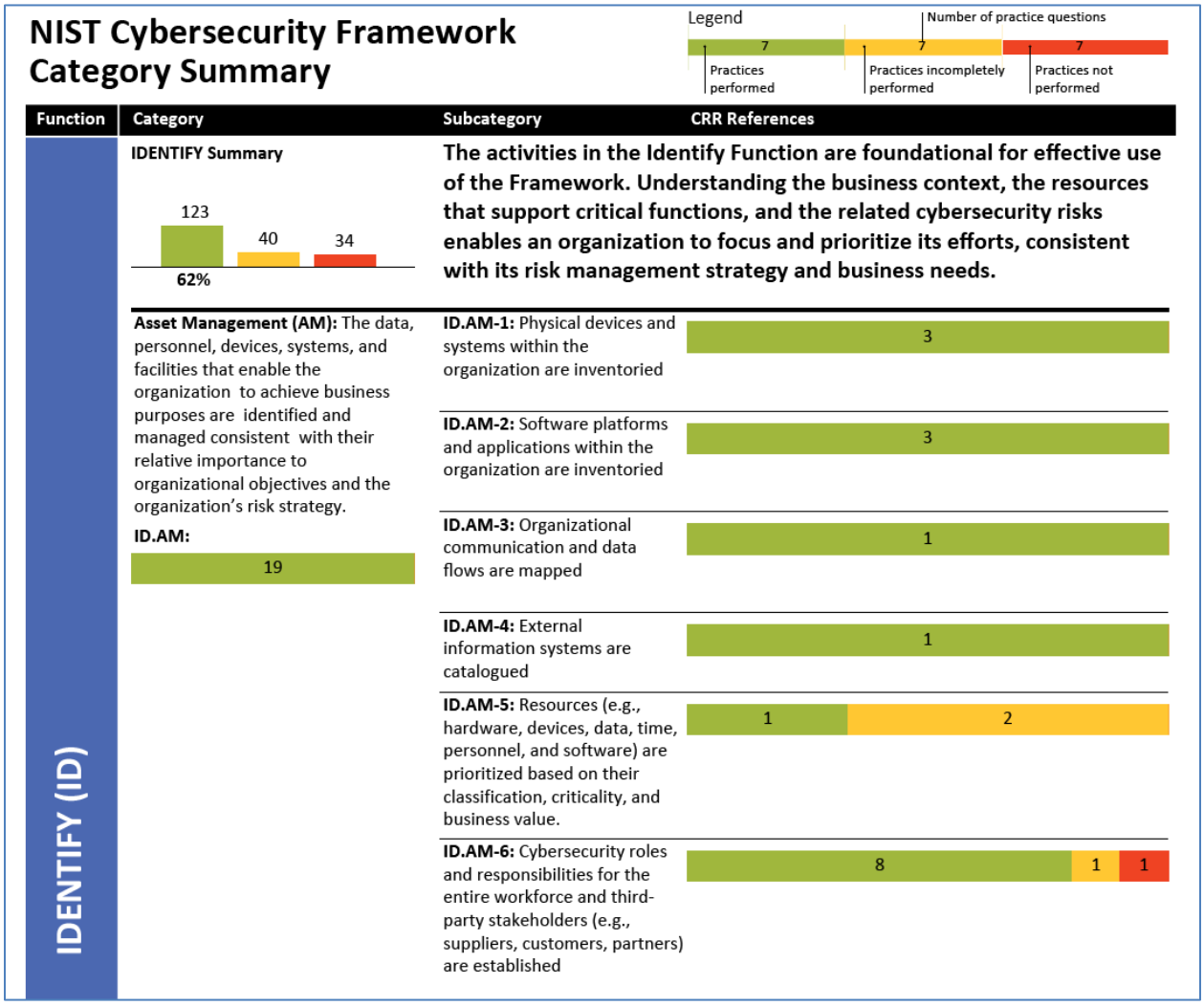

Figure 21: NIST Cybersecurity Framework Category Summary

An organization can also use the NIST Cybersecurity Framework Category Performance depiction (Figure 22) 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 CRA practices are mapped to specific CSF categories and subcategories.

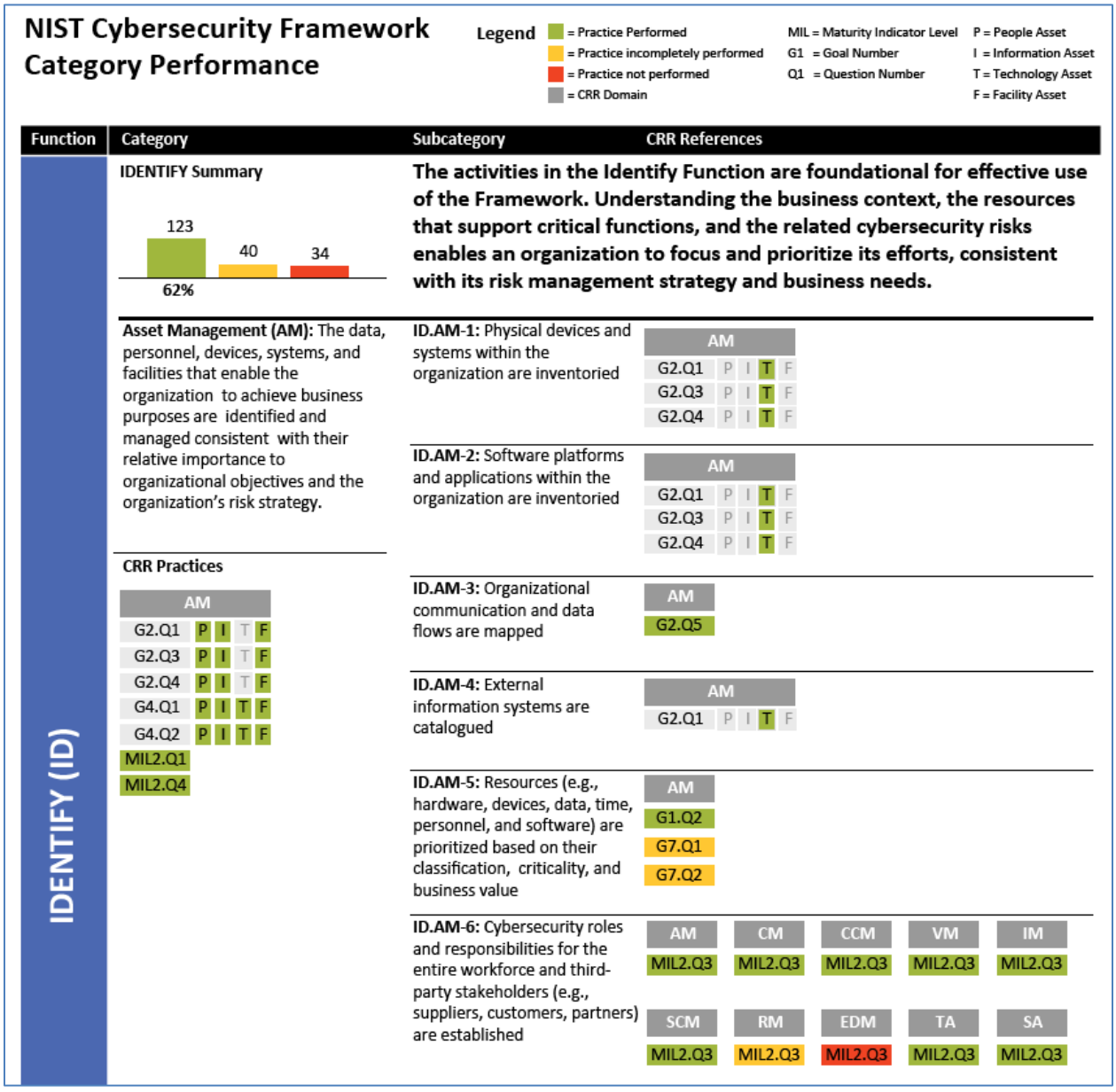

Figure 22: NIST Cybersecurity Framework Category Performance

Options for Consideration

The CRA Self-Evaluation 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 23).

CYBER RESILIENCE
ANALYSIS

Q1	**CERT-RMM Reference** **[SC:SG4.SP2]** Review plans to determine plan conflicts. Determine the severity of plan conflicts and develop appropriate mitigation actions to reduce or eliminate the conflicts. Conflicts that would impede successful plan execution pose operational risks that must be mitigated by the organization. Remember that the conflict may affect more than one plan, and therefore mitigation actions may have to be performed on more than one plan. **Additional References** NIST CSF References: PR.IP-9, RC.IM; NIST SP 800-171 References: 3.6.1	

Figure 23: Option for Consideration

Options for Consideration are primarily sourced from the CERT-RMM and NIST special publications. Appendix C of this guide gives a full list of sources. The CERT-RMM options contain a root reference to the relevant specific goals and practices. This root reference has a standard pattern of abbreviation: *process area:specific goal.specific practice.* In Figure 23, the CERT-RMM reference for Question 1 (Q1) is to Service Continuity:Specific Goal 2.Specific Practice 1.

4.3 Cyber Hygiene

Like personal hygiene, cyber hygiene should start with the basic actions that are most likely to promote good health. The CRA approach to cyber hygiene involves identifying the commonalities among the many existing sources of cyber hygiene practices and aligning them with the resilience management practices in the CERT Resilience Management Model (CERT-RMM). [3] Since the CRA is a derivative work product of the CERT-RMM, we can identify the practices in each CRA domain that would be considered cyber hygiene practice. It is recommended that organizations focus on the hygiene practices first if they have an immature cybersecurity program or if they are struggling to perform well in a particular domain. These practices help set the foundation for an organization's cybersecurity program.

The following cyber hygiene practices cover concepts that are paramount to every organization's success:

- Identify and prioritize key organizational services, products and their supporting assets.
- Identify, prioritize, and respond to risks to the organization's key services and products.
- Establish an incident response plan.
- Conduct cybersecurity education and awareness activities.
- Establish network security and monitoring.
- Control access based on least privilege and maintain the user access accounts.
- Manage technology changes and use standardized secure configurations.

[3] For more information about cyber hygiene, see the blog post *Cyber Hygiene: 11 Essential Practices* at https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html.

CYBER RESILIENCE
ANALYSIS

- Implement controls to protect and recover data.
- Prevent and monitor malware exposures.
- Manage cyber risks associated with suppliers and external dependencies.
- Perform cyber threat and vulnerability monitoring and remediation.

These 11 concepts manifest into approximately 80 CRA practices throughout the 10 CRA domains. A CRA cyber hygiene practice can be easily identified in the data capture form or the report section of the tool by looking for the "‡" symbol after the CERT-RMM reference as shown in Figure 24.

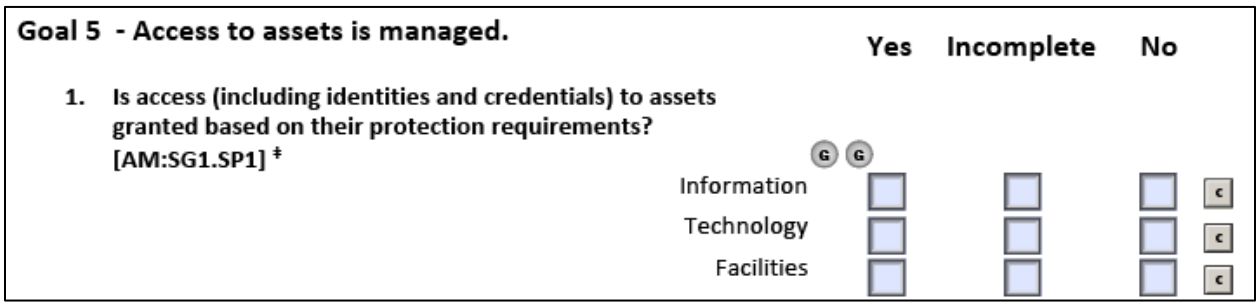

Figure 24: Cyber Hygiene Question Identification

4.4 Identify Gaps

The CRA Self-Evaluation 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 self-evaluation 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.

CYBER RESILIENCE
ANALYSIS

Table 5: Recommended Process for Using Results

	Inputs	Activities	Outputs
Perform Evaluation	1. CRA Self-Evaluation 2. Organizational policies and procedures 3. Understanding of current cybersecurity management and operations	1. Conduct the CRA Self-Evaluation	1. CRA Self-Evaluation Report
Analyze Identified Gaps	1. CRA Self-Evaluation 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 CRA 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 CRA does not prescribe the achievement of specific MILs for organizations in any particular sector. The CRA Self-Evaluation Report provides an organization with information on its current level of cybersecurity capabilities in each of the 10 CRA domains and can be used as a baseline for initiating a data-driven process improvement project, as depicted in Figure 25.

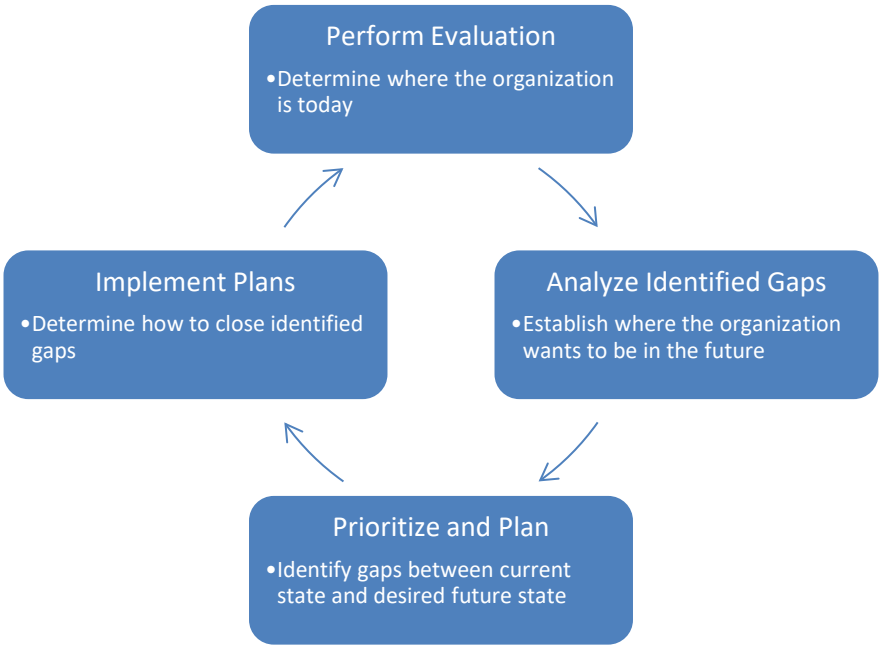

Figure 25: Steps in a Typical Process Improvement Activity

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

- Analyze Identified Gaps
- Prioritize and Plan
- Implement Plans

5.1 Analyze Identified Gaps

The CRA Self-Evaluation 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 CRA.

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

Setting a Target: Method 1

In this approach, an organization uses the results of a completed CRA analysis to jump-start the identification of its target state. The organization begins by walking through its scores in each domain of the CRA Self-Evaluation 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 self-evaluation 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 CRA practices before conducting an analysis 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 analysis to determine where gaps exist that need to be addressed.

CYBER RESILIENCE
ANALYSIS

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-analysis using the CRA Self-Evaluation Package can track progress toward the organization’s desired capability profile.

CYBER RESILIENCE
ANALYSIS

6 Summary

This document describes the Cyber Resilience Analysis (CRA) architecture and provides detailed descriptions of the 10 CRA domains and six Maturity Indicator Levels (MILs). This document also contains information about how to prepare for a CRA Self-Evaluation and how a facilitator assists the organization in evaluating 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 CRA Self-Evaluation Report.

The CRA Self-Evaluation also provides an analysis of an organization's capabilities relative to the NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", Cybersecurity Maturity Model Cerfitication (CMMC), and the NIST Cybersecurity Framework (CSF). A reference crosswalk for each NIST standard is included in the CRA Self-Evaluation Kit. Each reference crosswalk maps the relationship of the CRA goals and practices to the applicable NIST standard.

For additional assistance, the facilitator and other participants can contact the Department of Defense Cyber Crime Center (DC3) Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment at DCISE@dc3.mil.

CYBER RESILIENCE
ANALYSIS

Appendix A: Process Checklist

CRA Self-Evaluation Checklist

Purpose: To guide the CRA Self-Evaluation process

Time	Item	Description	Completed
Four weeks prior to self-evaluation workshop	Preparation meeting	Hold a preparation meeting. • Answer organizational questions. • Establish the scope of the analysis. • Identify participants. • Schedule the self-evaluation workshop.	☐
Two weeks prior to self-evaluation workshop	Facilities	Ensure that facilities have been set up correctly. • The room for the self-evaluation 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 higher or Adobe Acrobat.	☐
	Catering	Confirm catering, as applicable.	☐
One week prior to self-evaluation workshop	Availability	Confirm that all participants are available and committed to attend the workshop.	☐

Name	Title	Role (CRA Domain)
		AM
		CM
		CCM
		VM
		IM
		SCM
		RM
		EDM
		TA
		SA

CYBER RESILIENCE ANALYSIS

	Sponsor	Confirm that the sponsor is prepared to deliver opening remarks or has delegated this responsibility to another executive.	☐
After the self-evaluation workshop	Interpreting CRA Self-Evaluation Report	Examine the CRA Self-Evaluation Report and answer the following questions: • What are the overall strengths and weaknesses (see the Overall CRA 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? • 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 CRA Self-Evaluation 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 self-evaluations to measure progress. • Manage progress against the plan. • Re-plan as necessary.	☐

CYBER RESILIENCE
ANALYSIS

Appendix B: CRA Glossary/Terms

Term	Definition	Source
asset (organizational asset)	Something of value to an organization; typically, people, information, technology, and facilities that the critical services relies on. One of the foundational principles of the CRA 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 CRA. The purpose of asset management is to identify, document, and manage assets during their lifecycle to ensure sustained productivity to support critical services.	CRA
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 CRA. The purpose of configuration and change management is to establish processes to ensure the integrity of assets using configuration and change control audits.	CRA
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
Controls Management (CM)	A domain of practice within the CRA. The purpose of controls management is to identify, analyze, and manage controls in a critical service's operating environment.	CRA

CYBER RESILIENCE ANALYSIS

Term	Definition	Source
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.	CRA
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 CRA structure, a domain is a logical grouping of cybersecurity practices that contribute to the cyber resilience of an organization.	CRA
enterprise	The largest (i.e., highest level) organizational entity to which the organization participating in the CRA 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 CRA. 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.	CRA
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
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 CRA.	Adapted from CERT-RMM

CYBER RESILIENCE
ANALYSIS

Term	Definition	Source
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 CRA. The purpose of incident management is to establish processes to identify and analyze IT events, detect cybersecurity incidents, and determine an organizational response.	CRA
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
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.	CRA

CYBER RESILIENCE
ANALYSIS

Term	Definition	Source
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 to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT-RMM (monitoring and risk management)
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
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.	CRA
resilience	See *operational resilience*.	

CYBER RESILIENCE
ANALYSIS

Term	Definition	Source
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.	CRA
risk	The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty.	CERT-RMM
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 CRA. 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.	CRA
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 CRA. 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.	CRA

CYBER RESILIENCE ANALYSIS

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 CRA. 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.	CRA
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 CRA. 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.	CRA
vulnerability	An exposure, flaw, or weakness that could be exploited. The susceptibility of an organizational service or asset to disruption.	CERT-RMM

CYBER RESILIENCE
ANALYSIS

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

CYBER RESILIENCE
ANALYSIS

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

CYBER RESILIENCE
ANALYSIS

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

Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"
https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

Cybersecurity Maturity Model Certification
https://www.acq.osd.mil/cmmc/index.html