DoD CYBER CRIME CENTER

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

CYBER RESILIENCE ANALYSIS

Question Set and Guidance

JULY 2024

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.

DM24-0449

CYBER RESILIENCE **ANALYSIS**

Table of Contents

CYBER RESILIENCE
ANALYSIS

1 Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their lifecycle to ensure sustained productivity to support critical services.

Goals and Practices

Goal 1 – Services are identified and prioritized.

1. Are services identified? [SC:SG2.SP1]

Question Intent: To determine if **services are identified.**

- A **service is a set of activities** that the organization carries out in the **performance of a duty** or in the **production of a product.**
- **Services** can be **externally or internally focused. Examples can include:**
  - a customer-facing website such as an online payment system
  - human resources transactions
- A fundamental operational resilience objective is to **focus on activities to protect and sustain the identified services and assets** that most directly affect the organization's ability to achieve its mission.

Criteria for "Yes" Response:

- *The organization has **identified all services.***

Criteria for "Incomplete" Response:

- *The organization has identified **some** services.*

2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]

Question Intent: To determine **if services are prioritized based on analysis of the potential impact if the services are disrupted.**

- The organization should conduct analysis of identified services (e.g., a business impact analysis) to determine the impact to the organization of the loss or disruption of each service.
- The results of this analysis should then be used to prioritize the organizational services.

Typical work products:

- results of risk assessment and business impact analyses
- prioritized list of organizational services, activities, and associated assets

Criteria for "Yes" Response:

- *The organization has **prioritized all services** (identified in G1:Q1).*

Criteria for "Incomplete" Response:

- *The organization has prioritized some services.*

3. Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified and communicated? [EF:SG1.SP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if the **organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, is identified and communicated.**

- An organization's **strategic objectives include mission, vision, and values.** Effective operational resilience ensures the organization can accomplish these strategic objectives.
- **Specific objectives are goal oriented and outline the targets** the organization is attempting to reach. For example:
  - opening 100 stores
  - improving revenue by 14 percent
- The organization's **mission, vision, values, as well as the organization's place in critical infrastructure should be readily available in company literature** such as employee handbooks and annual reports.
- **Mission, vision, values, and the organization's place in critical infrastructure should be effectively communicated.**

Typical work products:

- organizational strategic objectives
- organizational mission, vision, values, and purpose statement

Criteria for "Yes" Response:

- *The organization has **documented** its mission, vision, values, and purpose, including its role in critical infrastructure, and **communicated** them.*

Criteria for "Incomplete" Response:

- *The organization's mission, vision, values, and purpose are **in development and partially documented**.*

4. Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP1]

Question Intent: To determine if **the organization prioritizes its mission, objectives, and activities.**

- The organization should **prioritize** its mission, objectives, and activities **to ensure the organization remains operationally resilient.**
- The **high-value services of the organization directly support the achievement of the organization's mission and objectives** and therefore must be protected and sustained to the extent necessary to minimize disruption.

Typical work products

- prioritized list of organizational mission, objectives, and activities

Criteria for "Yes" Response:

- *The organization **documents the prioritization** of its mission, objectives, and activities.*

Criteria for "Incomplete" Response:

- *The prioritization is **in development and partially documented**.*

Goal 2 – Assets are inventoried, and the authority and responsibility for these assets is established.

1. Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if the **assets that support the critical service are inventoried.**

- The organization should **inventory the assets** (people, information, technology, and facilities) **required for the delivery of the critical service**.
- Inventories of assets may **exist in multiple forms or physical locations**.

Criteria for "Yes" Response:

- *The organization **inventories all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization inventories **some** assets.*

2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]

Question Intent: To determine if **asset descriptions include protection and sustainment requirements.**

- Including protection and sustainment requirements in asset descriptions **provides a common source for communicating and updating** those requirements.
- The confidentiality, integrity, and availability requirements of the service are used to **derive the collective protection and sustainment requirements** of associated assets.
- Activities that implement **protection and sustainment requirements often appear as** processes, procedures, policies, controls, and plans.
- **Protection requirements** describe how an asset's exposure to sources of disruption and to the exploitation of vulnerabilities must be minimized. Examples include:
    - People – Ensure all employees are skilled in their role to protect against accidental disruption.
    - Information – All information assets will be disposed of according to policy to prevent unintentional disclosure.
    - Technology – All network boundaries should be protected using approved methods and tools to deny unauthorized access.
    - Facilities – Physical access to all service related information and technology assets must be limited to approved personnel to protect against accidental and malicious disruption.
- **Sustainment requirements** describe how assets must be kept operating when faced with disruptive events. Examples include:
    - People – All critical personnel shall have a designated backup who can fulfill their service continuity role.
    - Information – No more than 4 hours of the critical service data can be lost to ensure the continuity of the service.
    - Technology - The technology assets required for the delivery of the critical service must be operational within 48 hours to ensure the continuity of the service.
    - Facilities – The backup facility must meet the service continuity requirements of the critical service.

Criteria for "Yes" Response:

- *The organization **documents protection and sustainment requirements in asset descriptions** for **all assets** supporting the critical service.*

Criteria for "Incomplete" Response:

- *The organization documents protection and sustainment requirements in asset descriptions for **some** assets.*

3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]

Question Intent: To determine if **owners and custodians of assets are documented** in asset descriptions.

- Asset **owners** are the people or organizational entities, internal or external to the organization, that **have primary responsibility for the viability, productivity, and resilience of the asset.** Example asset owners include:
  - service owners
  - managers and staff supervisors
  - organizational units
  - lines of business
- Asset **custodians** are people or organizational entities, internal or external to the organization, who are **responsible for satisfying the protection and sustainment requirements for the asset established by the asset owner.** Example asset custodians include:
  - system/database administrator
  - facility manager
  - IT support organization
  - contractors hosting and managing data (e.g., cloud service provider)

Criteria for "Yes" Response:

- *The organization **documents owners and custodians in asset descriptions for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization documents owners and custodians in asset descriptions for **some** assets.*

4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]

Question Intent: To determine if the **physical locations of assets are documented** in the asset inventory.

- Physical **locations of assets can be internal or external** to the organization.
- The **location details should be sufficient enough to support the resilience requirements** of the service.

Criteria for "Yes" Response:

- *The organization **documents the location of all assets** that support the critical service in the asset inventory.*

Criteria for "Incomplete" Response:

- *The organization documents the location of **some** assets in the asset inventory.*

5. Are organizational communications and data flows mapped and documented in the asset inventory? [ADM:SG1.SP2]

Question Intent: To determine if **organizational communications and data flows** are **mapped and documented** in the asset inventory.

NIST 800-53 Rev.4 AC-4, CA-3, CA-9, PL-8:

- **Information flow control regulates where information is allowed to travel** within an information system and between information systems.
- **Dedicated connections** between information systems **should be authorized.**
- The **interconnection interface characteristics, security requirements,** and the nature of the communication should be **documented.**
- **Data flows include actions performed by users and processes acting on behalf of users.**

Criteria for "Yes" Response:

- *Organizational **communications and data flows are mapped and documented** in the asset inventory for **all** technology assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Organizational communications and data flows are mapped and documented in the asset inventory for **some** technology assets.*

Goal 3 – The relationship between assets and the services they support is established.

1. Are the associations between assets and the critical service they support documented? [ADM:SG2.SP1]

Question Intent: To determine if the **associations between assets and the critical service they support are documented.**

- **Associating assets in the asset inventory to services** helps the organization to determine where critical dependencies exist, validate resilience requirements, and develop and implement resilience strategies in support of the critical service.

Criteria for "Yes" Response:

- *The organization **documents associations between assets and the critical service for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization documents associations between assets and the critical service for **some** assets.*

2. Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]

Question Intent: To determine if **confidentiality, integrity, and availability requirements are established** for each service-related asset.

- The confidentiality, integrity, and availability requirements of the service **are used to derive** the collective protection and sustainment requirements of associated assets.
- Asset-level **requirements should be based on** the **deployment in, contributions to**, and the support of the critical service.

Criteria for "Yes" Response:

- *The organization **establishes confidentiality, integrity, and availability requirements for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization establishes confidentiality, integrity, and availability requirements for **some** assets.*

Goal 4 – The asset inventory is managed.

1. Have change criteria been established for asset descriptions? [ADM:SG3.SP1]

Question Intent: To determine if **change criteria have been established** for asset descriptions.

- The organization should have a **set of criteria to identify when changes to assets** affect the delivery of the critical service and **require a change to the asset description**.
- Change criteria should be **applied consistently** across all asset types.

Examples of triggers that can affect high-value assets:

- changes in services affecting the assets on which they rely (e.g., changes in availability requirements)
- changes in technology infrastructure and configuration
- creation or alteration of information
- contracts that the organization enters into that would identify new assets
- changes in organizational structure and staff—termination or transfer of staff between organizational units or changes in roles and responsibilities
- real-estate transactions that add, alter, or change existing facilities
- acquisition of assets such as technology or facilities

Criteria for "Yes" Response:

- *The organization has **established asset description change criteria for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has established asset description change criteria for **some** assets.*

2. Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]

Question Intent: To determine if **asset descriptions are updated when changes to assets occur.**

- **When changes to assets occur, asset descriptions should be updated** to ensure that current protection and sustainment strategies continue to be satisfied.

Typical work products:

- asset change documentation
- asset inventory status
- updated asset and service resilience requirements
- updated asset and service protection strategies and controls
- updated strategies and continuity plans for sustaining assets and services

Criteria for "Yes" Response:

- *When changes to assets occur, **asset descriptions are updated for all changed assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *When changes to assets occur, asset descriptions are updated for **some** changed assets.*

Goal 5 – Access to assets is managed.

1. Is access (including identities and credentials) to assets granted based on their protection requirements? [AM:SG1.SP1]

Question Intent: To determine if access to **assets is granted based on their protection requirements.**

- **Protection requirements** describe how an assets exposure to sources of disruption and to the exploitation of vulnerabilities must be minimized.

CYBER RESILIENCE **ANALYSIS**

- **Access requests** should be **granted in accordance with the protection requirements** that have been established for the asset.
- **Access privileges are assigned and approved by asset owners** based on the role of the person, object, or entity that is requesting access.

Typical work products:

- asset protection requirements
- access requests
- access approval
- access control policy
- access rights and responsibilities

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within CMMC / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Practice		
AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC.L1-3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC.L2-AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.
CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.	IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	MP.L2-3.8.2 Limit access to CUI on system media to authorized users.
PE.L1-3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	

Criteria for "Yes" Response:

- ***Access to assets is granted based on their protection requirements, for all assets*** *that support the critical service.*
- ***The types of transactions and functions that authorized users are permitted to execute are defined,*** *and* ***system access is limited to the defined types of transactions and functions for authorized users.***
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Practices listed in the guidance for this practice are implemented, addressed, or considered in the context of the practice.***

Criteria for "Incomplete" Response:

- *Access to assets is granted based on their protection requirements, for* ***some*** *assets.*

2. Are access (including identities and credentials) requests reviewed and approved by the asset owner? [AM:SG1.SP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if **access requests are reviewed and approved by the asset owner.**

- **Asset owners** are responsible for reviewing the access request and the asset's protection requirements to decide whether to **approve or deny access.**
- The **access provided should** be commensurate with and **not exceed the requestor's job responsibilities.**
- If the **custodian of the asset is different from the owner**, the owner should **communicate in writing the approval for the request.**

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within CMMC / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC.L1-3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC.L2-AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.
CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.	IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	MP.L2-3.8.2 Limit access to CUI on system media to authorized users.
PE.L1-3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	

Criteria for "Yes" Response:

- ***All access requests*** *for assets that support the critical service* ***are reviewed and approved by the asset owner****.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice****.*

Criteria for "Incomplete" Response:

- ***Some*** *access requests for assets that support the critical service are reviewed and approved by the asset owner.*

3. Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3]

Question Intent: To determine if **access privileges are reviewed to identify excessive or inappropriate privileges.**

- **Periodic review** (as defined by the organization) of access privileges is the primary **responsibility of the asset owners.**
- Reviews should identify privileges that are:
    - excessive and in violation of the asset's resilience requirement
    - out of alignment with the identity's role or job responsibility
    - assigned but never approved by the asset owner

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC.L1-3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
AC.L2-AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.	IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.
MP.L2-3.8.2 Limit access to CUI on system media to authorized users.	PE.L1-3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	SC.L2-3.13. Prevent unauthorized and unintended information transfer via shared system resources.

Criteria for "Yes" Response:

- ***All assets*** *that support the critical service* ***are reviewed to identify excessive or inappropriate access privileges****.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice****.*

Criteria for "Incomplete" Response:

- ***Some*** *assets that support the critical service are reviewed to identify excessive or inappropriate access privileges.*

4. Are access privileges modified as a result of reviews? [AM:SG1.SP4]

Question Intent: To determine if **access privileges are modified as a result of the reviews.**

- Excessive or inappropriate levels of **access privileges must be corrected in a timely manner** to avoid exposing the organization to additional risk.
- As a result of periodic review, **asset owners may authorize custodians to make modifications such as**:
  - change or disable certain privileges to preserve resilience requirements
  - disable an access account that is no longer valid

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC.L1-3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
AC.L2-AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.	IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.
MP.L2-3.8.2 Limit access to CUI on system media to authorized users.	PE.L1-3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

Criteria for "Yes" Response:

- ***Access privileges are modified*** *as a result of reviews* ***for all assets*** *that support the critical service.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice****.*

Criteria for "Incomplete" Response:

- *Access privileges are modified as a result of reviews for* ***some*** *assets.*

5. Are access permissions managed incorporating the principle of least privilege? [AM.SG1.SP1]

Question Intent: To determine if **access permissions are managed in accordance with the principle of least privilege.**

NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16:

- The identification of authorized users and the specification of access privileges reflect the requirements of the critical service.
- **Access control policies** control access between users (or processes acting on behalf of users) and information systems.
- Access permissions can also be employed at the application and service level to provide increased information security.
- The principle of **least privilege** is employed to ensure users and processes operate at privilege levels no higher than necessary.

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within CMMC / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Practice		
AC.L2-3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC.L2-3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
SC.L2-3.13.3 Separate user functionality from system management functionality.	SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	

Criteria for "Yes" Response:

- ***Access permissions*** *for* ***all*** *assets that support the critical service are* managed in accordance with the principle of least privilege*.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Practices*** *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice.***

Criteria for "Incomplete" Response:

- *Access permissions for* ***some*** *assets that support the critical service are managed in accordance with the principle of least privilege.*

6. Are access permissions managed incorporating the principle of separation of duties? [AM.SG1.SP1]

Question Intent: To determine if **access permissions are managed in accordance with the principle of separation of duties.**

NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16:

- The identification of authorized users and the specification of access privileges reflect the requirements of the critical service.
- **Access control** policies control access between users (or processes acting on behalf of users) and information systems.
- **Separation of duties** addresses the potential for abuse of authorized privileges by **dividing roles and privileges between users** (e.g., ensuring security personnel administering access control functions do not also administer audit functions).

Criteria for "Yes" Response:

- ***Access permissions** for **all** assets that support the critical service are **managed in accordance with the principle of separation of duties**.*

Criteria for "Incomplete" Response:

- *Access permissions for **some** assets that support the critical service are managed in accordance the principle of separation of duties.*

7. Are identities (e.g., user accounts) proofed before they are bound to credentials that are asserted in interactions? [ID:SG1.SP1]

Question Intent: To determine if **identities are proofed before they are bound to credentials that are asserted in interactions**.

NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

NIST 800-63a – Digital Identify Guidelines:
An **identity** documents the existence of a person, object, or entity that requires access to organizational assets, such as information, technology, and facilities, to fulfill its role in executing services. An entity may be both internal and external to the organization.

Requiring multiple forms of identification, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity.

In-person registration could reduce the likelihood of fraudulent identifiers being issued by requiring the physical presence of individuals and actual face-to-face interactions with designated registration authorities.

- A subject (e.g., employee or user) requesting access to an asset is provided a unique digital identity (e.g., user account).
- Before providing the subject with a digital identity, organizations should conduct identity proofing:
  - Verify that the claimed identity is associated with the real person supplying the identity evidence, which can include
    - name
    - address
    - date of birth
    - email

  - phone number
  - Social Security number

  - Validate the subject's identity evidence against an authoritative source.
- Once the subject's identity is proofed, credentials (e.g., authenticators) are bound to the identity.
  - Authenticators include passwords, biometrics, etc.
- Identities should be asserted in network interactions to provide non-repudiation (i.e., associate action or changes with a unique individual).

Criteria for "Yes" Response:

- ***All identities*** *used to access* ***any asset that supports the critical service are proofed*** *before being bound to credentials that are asserted in interactions.*

Criteria for "Incomplete" Response:

- ***Some identities*** *used to access* ***any asset that supports the critical service are proofed*** *before being bound to credentials that are asserted in interactions.*

Goal 6 – Information assets are categorized and managed to ensure the sustainment and protection of the critical service.

1. Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)? [KIM:SG1.SP2]

Question Intent: To determine if **information assets are categorized based on sensitivity and potential impact to the critical service.**

- Categorizing information assets based on sensitivity and potential impact to the critical service **allows an organization to properly label the information assets and provide an appropriate level of protection.**
- The **sensitivity categorization scheme should cover all information assets** that support the critical service.
- **Sensitivity categorization** is a characteristic of an information asset that **should be documented** as part of the information asset inventory.

Examples of information asset sensitivity categories:

- public or non-sensitive
- restricted or internal use only
- confidential or proprietary (organizational intellectual property, product designs, customer information, employee records)
- privacy (e.g., PII, PHI)

Criteria for "Yes" Response:

- ***All information assets*** *that support the critical service* ***are categorized based on the sensitivity and potential impact to the critical service****.*

Criteria for "Incomplete" Response:

- ***Some*** *information assets that support the critical service are categorized based on the sensitivity and potential impact to the critical service.*

2. Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]

Question Intent: To determine if the **categorization of information assets is monitored and enforced.**

- The organization should **monitor the categorization of information assets** using techniques such as audits or spot-check inspections to ensure that the **approved methods of information categorization are being followed.**

Criteria for "Yes" Response:

- *The organization **monitors and enforces the categorization of all information** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization monitors and enforces the categorization of **some** information assets.*

3. Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]

Question Intent: To determine if **policies and procedures for the proper labeling and handling of information assets exist.**

- The **labeling and handling of information assets** should be **defined** and communicated through **policy**.
- Procedures should **address how to label and handle the information assets** to satisfy policy.
- **Labeling includes the required privacy and security notices** consistent with the data categorization (e.g. CUI).

Criteria for "Yes" Response:

- *There are **documented policies and procedures** for the proper labeling and handling of all information assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Policies and procedures are **in development and partially document**.*

4. Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories? [KIM:SG1.SP2]

Question Intent: To determine **if all staff members who handle information assets are trained** in the use of information categories.

- The organization should **train staff** (including those who are external to the organization) **on the approved methods of categorizing, labeling, and handling of information assets.**
- **Training the staff supports the consistent application of the categorization scheme** and the consistent handling of information assets across the organization.

Criteria for "Yes" Response:

- ***All staff members** (including those external to the organization) who handle information assets that support the critical service **are trained in the proper use of information categories**.*

Criteria for "Incomplete" Response:

- ***Some staff members** who handle information assets that support the critical service **are trained in the proper use of information categories.***

5. Are high-value information assets backed-up and retained? [KIM:SG6.SP1]

Question Intent: To determine **if high-value information assets are backed-up and retained.**

- High-value **information assets should be backed-up and retained to meet the protection and sustainment requirements** of the critical service.
- The organization should consider the following when backing up information assets:
  - protection and sustainment requirements for the critical service
  - frequency of backup and storage
  - retention period
  - acceptable back-up and retention media
  - accessing information back-ups

Criteria for "Yes" Response:

- ***All high-value information assets*** *that support the critical service* ***are backed-up and retained.***

Criteria for "Incomplete" Response:

- ***Some*** *high-value information assets are backed-up and retained.*

6. Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]

Question Intent: To determine if **guidelines exist for properly disposing of information assets.**

- Properly disposing of information assets is necessary to ensure that there are no unauthorized disclosures.
- Disposal **guidelines can apply to asset decommissioning, removal or sanitizing for reuse**.
- **Guidelines** for the disposal of information assets should consider:
  - confidentiality requirements
  - sensitivity categorization
  - applicable rules, laws, and regulations

Criteria for "Yes" Response:

- *There are* ***documented guidelines*** *for properly disposing of information assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Guidelines are* ***in development and partially documented****.*

7. Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]

Question Intent: To determine if **adherence to information asset disposal guidelines is monitored and enforced.**

- The **organization should provide oversight**, such as audits or spot-check inspections to ensure that the approved methods of information disposal are being followed.

Criteria for "Yes" Response:

- *The organization* ***monitors and enforces adherence to disposal guidelines for all information assets*** *that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization monitors and enforces adherence to disposal guidelines for* ***some*** *information assets.*

CYBER RESILIENCE **ANALYSIS**

Goal 7 – Facility assets supporting the critical service are prioritized and managed.

1. **Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities? [EC:SG1.SP1]**

Question Intent: To determine if **facilities are prioritized based on potential impact to the critical service.**

- **Prioritization** should be used to identify the facilities that should be the focus of protection and sustainment activities.

Example criteria for the establishment of high-priority facility assets can include:

- the use of the facility asset in the general management and control of the organization (corporate headquarters, primary data centers, etc.)
- facility assets that support more than one critical service
- the value of the asset in directly supporting the organization's delivery of the critical service

Criteria for "Yes" Response:

- *The organization **prioritizes all facility assets** that support the critical service **based upon their potential impact to the critical service**.*

Criteria for "Incomplete" Response:

- *The organization prioritizes **some** facility assets that support the critical service.*

2. **Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]**

Question Intent: To determine if **the prioritization of facilities is reviewed and validated.**

- **Periodic review and validation of the prioritization of facilities is needed** to account for operational and organizational environment changes**.**

Criteria for "Yes" Response:

- *The organization **reviews and validates the prioritization of all facility assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization reviews and validates the prioritization of **some** facility assets.*

3. **Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]**

Question Intent: To determine if **protection and sustainment requirements** of the critical service **are considered during the selection of facilities.**

- The confidentiality, integrity, and availability requirements of the service are used to **derive the collective protection and sustainment requirements of associated facility assets**.
- **Protection requirements** describe how an asset's exposure to sources of disruption and to the exploitation of vulnerabilities must be minimized.
- **Sustainment requirements** describe how assets must be kept operating when faced with disruptive events.
- Protecting facility assets from vulnerabilities, threats, and risks requires the organization to **develop appropriate protection and sustainment requirements.**

Example protection and sustainment requirements to consider include:

- geographic location – proximity to flood zones, earthquake zones
- security of the facility – physical barriers, physical access controls
- environmental conditions – electromagnetic radiation, heating and cooling
- availability of support utilities - water, sewage, electricity, gas supplier
- fire suppression
- communications infrastructure availability
- backup power generation

Criteria for "Yes" Response:

- *The organization **considers the protection and sustainment requirements** of the critical service **when selecting all facility assets** that will support the critical service.*

Criteria for "Incomplete" Response:

- *The organization considers the protection and sustainment requirements of the critical service when selecting **some** facility assets that will support the critical service.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing asset management activities? [ADM:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** asset management activities **exists.**

- The plan defines asset management within the organization and **prescribes how asset management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- asset management activities (service identification and prioritization, asset identification, management of the asset inventory, access control, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing asset management.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for asset management? [ADM:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** asset management activities **exists.**

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the asset management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform asset management activities
- establishment of procedures, standards, and guidelines
- establishing and maintaining an asset inventory
- managing access to assets
- categorizing, safeguarding, and disposing of information assets
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing asset management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for asset management activities been identified and made aware of their roles? [ADM:GG2:GP7]

Question Intent: To determine if **stakeholders** for asset management activities have been **identified** and **made aware of their roles.**

Stakeholders of the asset management process have the following **responsibilities:**

- creating an asset inventory baseline
- associating assets with the critical service
- overseeing the asset management process
- managing the risk resulting from unresolved problems (gaps in the inventory of asset protection and sustainment requirements, insufficient staffing or funding, etc.)

Examples of stakeholders include:

- critical service owners
- asset management staff
- owners and custodians of assets that underpin the service (to include facility security personnel)
- critical service staff

- external entities responsible for some part of the service
- information technology staff
- human resources
- internal and external auditors

Criteria for "Yes" Response:

- ***All*** *stakeholders for the asset management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the asset management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but have* ***not been made aware*** *of their roles.*

4. Have asset management standards and guidelines been identified and implemented? [ADM:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing asset management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **asset management activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- establishing an asset inventory
- documenting asset descriptions and relevant information
- identifying asset owners
- identifying asset custodians
- assigning access to assets
- sensitivity categorization for information assets
- documenting asset resilience requirements

Criteria for "Yes" Response:

- *The organization has* ***implemented documented standards and guidelines*** *for performing asset management activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented.***

MIL3-Managed

1. Is there management oversight of the performance of the asset management activities? [ADM:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the asset management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the asset management activities.

- **Oversight** provides **visibility** into the asset management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products (access control lists, outdated asset profiles, excessive access privileges, improper disposal of sensitive information, etc.) or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the asset management activities
- escalating issues that require higher-level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day asset management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day asset management activities.*

2. Have qualified staff been assigned to perform asset management activities as planned? [ADM:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan.**

- Qualified means that **staff are appropriately skilled** to perform asset management activities.

Examples of staff include personnel responsible for:

- developing and maintaining the asset inventory, including asset profiles
- identifying asset's dependencies
- documenting changes to assets in the asset inventory
- implementing processes, standards, and guidelines
- addressing issues and problems, including developing and executing remediation plans

Examples of skills needed include:

- knowledge of the tools, techniques, and methods necessary to identify and inventory assets
- knowledge necessary to identify, document, and manage assets through their lifecycle
- knowledge of sensitivity categories for information assets

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned asset management activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff** assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform asset management activities as planned? [ADM:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided.** The intent of the question is to **evaluate** the completeness of the **funding, not the completeness of the plan.**

- **Funding** is an indication of higher-level management support and sponsorship of asset management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned asset management activities include:

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned asset management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled? [ADM:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the asset management activities.

- The intent is to **determine risks that prevent the organization from performing asset management activities** (asset management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the asset management process include:

- poorly defined asset management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned asset management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of **some** of the planned asset management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned asset management activities are **identified, but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. **Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results? [ADM:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **asset management activities (process) remain effective** and **produce intended results** by **periodic review and measurement.**

Periodic (as defined by the organization) reviews of the asset management process are needed to ensure that:

- the asset inventory is up to date
- excessive access to assets is identified and remediated
- the quality of particular work products meets established guidelines
- risk related to asset management problem areas are identified and addressed
- actions requiring management involvement are elevated in a timely manner

Example metrics of the asset management process may include:

- number of assets with incomplete asset profiles
- number of discrepancies between the current inventory and the documented inventory
- assets that do not have an assigned owner or custodian
- the level of adherence to the asset management plan and processes

Criteria for "Yes" Response:

- ***All** asset management activities are **periodically** (as defined by the organization) **reviewed** and **measured** and the **results evaluated**.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review of the asset management activities.*
- *Or; review and measurement addresses **some** of the asset management activities.*
- *Or; asset management activities are **reviewed but not measured**.*

2. **Are asset management activities periodically reviewed to ensure they are adhering to the plan? [ADM:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To **periodically** determine if asset management activities are being **performed as planned.**

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the asset management plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing asset management activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- ***All*** *asset management activities are* ***periodically (as defined by the organization) reviewed*** *to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review.*
- *Or;* ***some*** *asset management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of asset management? [ADM:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of asset management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues.**

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the asset management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes:

- **status reviews** of asset management activities
- **issues** identified in process and plan reviews
- **risks** associated with asset management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is* ***made aware of issues*** *related to the performance of asset management through* ***scheduled*** *communication.*

Criteria for "Incomplete" Response:

- *The organization has* ***not established a frequency*** *for communication to higher-level management.*
- *Or; communications address* ***some*** *issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances? [ADM:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines asset management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in asset management activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed

- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of asset management.*

Criteria for "Incomplete" Response:

- *A standard definition of asset management is **in development and partially documented**.*

2. Are improvements to asset management documented and shared across the organization? [ADM:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the asset management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the asset management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include:

- process metrics and measurements
- lessons learned from process reviews
- lessons learned in the post-event review of incidents and disruptions in continuity

Criteria for "Yes" Response:

- ***Improvements** to asset management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to asset management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

CYBER RESILIENCE
ANALYSIS

2 Controls Management

The purpose of Controls Management is to identify, analyze, and manage controls in a critical service's operating environment.

Goals and Practices

Goal 1 – Control objectives are established.

1. Have control objectives been established for assets required for delivery of the critical service? [CTRL:SG1.SP1]

Question Intent: To determine if **control objectives** for the critical service have been **established.** Control objectives are important because controls are designed to meet those objectives.

- **Control objectives** provide a set of high-level requirements for the protection and sustainment of a critical service and associated assets.
- **Sources** for identifying control objectives may be found in governance documents, policy documents, contractual requirements (NIST SP800-171), etc.

Asset Type	Control Objective Example
People	▪ Ensure all employees are trustworthy and reliable prior to hiring them. ▪ All outside support personnel are identified.
Information	▪ Ensure the confidentiality and integrity of customer's payment information. ▪ Information assets are disposed of according to policy.
Technology	▪ Ensure the databases that support one or more critical services remain available. ▪ Network integrity is protected.
Facilities	▪ Ensure environmental systems are maintained at an appropriate level to support datacenter equipment. ▪ Physical access to assets is managed and protected.

Criteria for "Yes" Response:

- *Control objectives are established for **all** assets (people, information, technology, and facilities).*
- *And; **all** control objectives are documented.*

Criteria for "Incomplete" Response:

- *Control objectives are established for **some** assets.*

2. Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]

Question Intent: To determine if control objectives are **prioritized**. The intent of prioritization is to determine the control objectives that are **most important** because of the **potential to affect the critical service** if the objective is not met.

- **Assigning a relative priority** to each control objective also aids in determining the level of resources to apply when defining, analyzing, assessing, and addressing gaps in controls.
- **Prioritization can be based on:** risk assessments, business impact analysis, etc.

CYBER RESILIENCE ANALYSIS

Criteria for "Yes" Response:

- ***All*** *control objectives (established in CTRL:G1.Q1) are prioritized.*
- *And; prioritization is* ***documented****.*
- *And; prioritization is* ***current*** *(periodic review as defined by the organization).*

Criteria for "Incomplete" Response:

- *Control objectives are prioritized for* ***some*** *assets (people, information, technology, and facilities).*

Goal 2 – Controls are implemented.

1. Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]

Question Intent: To determine if administrative, technical, and physical **controls are designed and implemented** to meet control objectives for the critical service.

Asset Type	Control Objective Example	Control Example
People	▪ Ensure all employees are trustworthy and reliable prior to them being hired. ▪ All outside support personnel are identified.	▪ Background check ▪ Visitor badges required for outside support personnel ▪ Visitors are escorted
Information	▪ Ensure the confidentiality and integrity of customer's payment information ▪ Information assets are disposed of according to policy.	▪ Encryption of customer payment data ▪ Provide secure disposal bins ▪ Monitor adherence to policy
Technology	▪ Ensure the databases, which support one or more critical services, remains available. ▪ Network integrity is protected.	▪ Fault tolerant architecture ▪ Implement network monitoring
Facilities	▪ Ensure environmental systems are maintained at appropriate level to support datacenter equipment. ▪ Physical access to assets is managed and protected.	▪ Establish preventative maintenance schedule ▪ Implement an access control system

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

CYBER RESILIENCE ANALYSIS

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.8 Limit unsuccessful logon attempts.	AC.L2-3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	AC.L2-3.1.11 Terminate (automatically) a user session after a defined condition.
IA.L2-3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA.L2-3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA.L2-3.5.5 Prevent reuse of identifiers for a defined period.
IA.L2-3.5.6 Disable identifiers after a defined period of inactivity.	IA.L2-3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.	IA.L2-3.5.8 Prohibit password reuse for a specified number of generations.
IA.L2-3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.	IA.L2-3.5.10 Store and transmit only cryptographically-protected passwords.	IA.L2-3.5.11 Obscure feedback of authentication information.
PE.L1-3.10.5 Control and manage physical access devices.	SC.L2-3.13.9 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 located directly below practice CM:G2.Q1 to select the CUI requirement that the organization implements. This information will allow the organization to accurately track the CUI requirements they have in place to focus on CUI requirements that are not implemented.

Criteria for "Yes" Response:

- *The organization has **implemented controls** to satisfy **all** the established control objectives.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements** 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.*

2. Have controls been implemented, incorporating network segregation where appropriate, to protect network integrity? [CTRL:SG2.SP1]

Question Intent: To determine if **controls** have been implemented to **protect network integrity using network segregation** where appropriate.

NIST 800-53 Rev.4 AC-4, SC-7:

- Methods to protect network integrity include implementation of:
  - firewalls
  - intrusion detection and prevention systems (IDS/IPS)
  - host-based intrusion detection
  - unidirectional gateways
  - vulnerability scanners
  - security information and event management (SIEM) systems
- **Segregation** is a form of boundary protection. Segregation is the **capability to isolate** or segregate certain organizational **information system assets.**
- Segregation **reduces the attack surface** of the information system and **provides the capability to more effectively control information flows. Segregation applies to both internal and external boundaries, and can be implemented using VLANs, firewalls, DMZs, etc.**

CYBER RESILIENCE **ANALYSIS**

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.14 Route remote access via managed access control points	SC.L1-3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC.L1-3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
SC.L2-3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC.L2-3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. (i.e. split tunneling).	

Criteria for "Yes" Response:

- ***Controls have been implemented to protect network integrity****, incorporating network segregation where appropriate, for* ***all*** *network (technology) assets that support the critical service.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect network integrity, incorporating network segregation where appropriate, for* ***some*** *network (technology) assets.*

3. Have controls been implemented to protect data-at-rest? [CTRL:SG2.SP1],[KIM:SG4.SP2]

Question Intent: To determine if **controls** have been implemented to **protect data-at-rest.**

NIST 800-53 Rev.4 SC-28:

- **Data-at-rest is information located on storage devices** that are components of information systems.
- This control addresses the **confidentiality and integrity** of data-at-rest.

System-related information that requires protection includes:

- configurations or rule sets for
  - firewalls
  - gateways
  - intrusion detection/prevention systems
  - routers

Mechanisms to achieve confidentiality and integrity protections include:

- encryption
- file share scanning
- write-once-read-many (WORM) technologies
- secure off-line storage
- access controls

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.	MP.L2-3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP.L2-3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards	MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations.	SC.L2-3.13.19 Establish and manage cryptographic keys for cryptography employed in organizational systems.
SC.L2-3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC.L2-3.13.16 Protect the confidentiality of CUI at rest.	

Criteria for "Yes" Response:

- ***Controls have been implemented to protect data-at-rest*** *for* ***all*** *information assets that support the critical service.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect data-at-rest for* ***some*** *information assets.*

4. Have controls been implemented to protect data-in-transit? [CTRL:SG2.SP1],[KIM:SG4.SP1],[KIM:SG4.SP2]

Question Intent: To determine if **controls** have been implemented to **protect data-in-transit.**
NIST 800-53 Rev.4 SC-8:

- The information system **protects** the confidentiality and/or integrity of **data-in-transit.**
- This control **applies to both internal and external networks** and all types of information system components from which information can be transmitted.

Mechanisms to achieve confidentiality and integrity protections include:

- encryption
- randomized communication patterns

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
3.1.3 Control the flow of CUI in accordance with approved authorizations.	3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	3.1.17 Protect wireless access using authentication and encryption.
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3.13.15 Protect the authenticity of communications sessions.	

Criteria for "Yes" Response:

- ***Controls have been implemented to protect data-in-transit*** *for* ***all*** *information assets that support the critical service.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect data-in-transit for* ***some*** *information assets.*

5. Have controls been implemented to protect against data leaks? [CTRL:SG2.SP1],[KIM:SG4.SP1],[KIM:SG4.SP2]

Question Intent: To determine if **controls** have been implemented to **protect against data leaks.**
NIST 800-53 Rev.4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4:

- **Information/data leakage** is the intentional or unintentional release of information to an untrusted environment.

Methods to protect against data leaks include:

- special cabling (emanation protection)
- access control
- encryption
- data leakage prevention (DLP)

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.3 Control the flow of CUI in accordance with approved authorizations.	AC.L2-3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC.L2-3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.
AC.L1-3.1.22 Control CUI posted or processed on publicly accessible systems	MP.L2-3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.
MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations.	PE.L2-3.10. Protect and monitor the physical facility and support infrastructure for organizational systems.	SC.L1-3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
SC.L2-3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.		

Criteria for "Yes" Response:

- ***Controls have been implemented to protect against data leaks*** *for* ***all*** *information assets that support the critical service.*
- *These* ***controls include identification of 1) individuals authorized to manage CUI on publicly accessible systems, 2) procedures to control posting / processing of same, 3) a pre-posting review process, and 4) removal of improperly posted CUI.***
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect against data leaks for* ***some*** *information assets.*

6. Have audit/log records been determined, documented, implemented, and reviewed in accordance with policy? [CTRL:SG2.SP1],[MON:SG1.SP3]

Question Intent: To determine if **audit/log records have been determined, documented, implemented, and reviewed** in accordance with policy.
NIST 800-53 Rev.4 AU Family:

- To **determine the set of auditable events**, organizations should **consider the auditing appropriate for each of the security controls** to be implemented.
- **To ensure that the current set of auditable events is still appropriate**, a periodic review should be performed.
- **Information system audit records** should be **periodically** (as defined by the organization) **reviewed** for indications of inappropriate or unusual activity.
- **Audit information and audit tools should be protected** from unauthorized access, modification, and deletion.
- Organizations should **retain audit records** until it is determined that they are no longer needed for administrative, legal, audit, or other purposes.

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AU.L2-3.3.1 Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	AU.L2-3.3.3 Review and update audited events.	AU.L2-3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.
AU.L2-3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU.L2-3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	PE.L1-3.10.4 Maintain audit logs of physical access.

Criteria for "Yes" Response:

- ***Audit/log records have been determined, documented, implemented, and reviewed in accordance with policy****, where appropriate, for* ***all*** *assets that support the critical service.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI***

Requirements *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice****.*

Criteria for "Incomplete" Response:

- *Audit/log records have been determined, documented, implemented, and reviewed in accordance with policy, where appropriate, for* ***some*** *assets.*

7. Have controls been implemented to protect and restrict the use of removable media in accordance with policy? [CTRL:SG2.SP1],[TM:SG2.SP2]

Question Intent: To determine if **controls** have been implemented to **protect and restrict the use of removable media** in accordance with policy.
NIST 800-53 Rev.4 MP-2, MP-4, MP-5, MP-7:

- Organizations may **restrict user access** to removable media to defined personnel or roles.
- Organizations may **restrict the use of certain types** of removable media.
- **Physically controlling** information system **media** includes:
  - conducting inventories
  - ensuring procedures are in place to allow individuals to check out and return media to the media library
  - maintaining accountability for all stored media
- The type of media **storage** should be **appropriate for the security category and/or classification** of the information residing on the media.
- **Media should be protected during transport** outside of controlled areas using established safeguards. Safeguards can include:
  - locked containers
  - encryption

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.21 Limit use of organizational portable storage devices on external systems.	MP.L2-3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP.L2-3.8.2 Limit access to CUI on system media to authorized users.
MP.L2-3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	MP.L2-3.8.7 Control the use of removable media on system components.
MP.L2-3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.		

Criteria for "Yes" Response:

- ***Controls have been implemented to protect and restrict the use of removable media*** *on* ***all*** *assets that support the critical service.*

- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect and restrict the use of removable media on* ***some*** *assets that support the critical service.*

8. Have controls been implemented to protect communication and control networks? [CTRL:SG2.SP1],[TM:SG2.SP2]

Question Intent: To determine if **controls** have been implemented **to protect communication and control networks.**

NIST 800-53 Rev.4 AC-4, AC-17, AC-18, CP-8, SC-7:

- Establish and document **usage restrictions, configuration/connection requirements, and implementation guidance** for:
  - each type of remote access allowed
  - wireless access
  - communication systems access (radios, phones, public address, etc.)
  - supervisory control and data acquisition (SCADA) and industrial control system (ICS)
- The organization **establishes alternate telecommunications services** for the critical service to use when the primary telecommunications capabilities are unavailable.
- **Connections** to communication or control systems are **implemented through managed interfaces.** Managed interfaces include:
  - gateways
  - routers
  - firewalls
  - encrypted tunnels

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.14 Route remote access via managed access control points	AC.L2-3.1.16 Authorize wireless access prior to allowing such connections.	AC.L2-3.1.17 Protect wireless access using authentication and encryption.
AC.L2-3.1.18 Control connection of mobile devices.	SC.L1-3.13. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC.L2-3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. (i.e. split tunneling).
SC.L2-3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	SC.L2-3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	

Criteria for "Yes" Response:

- ***Controls have been implemented to protect all communication and control network (technology) assets*** *that support the critical service.*

- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *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 to protect* ***some*** *communication and control network (technology) assets.*

9. Have cybersecurity human resource practices been implemented for the critical service (e.g., de-provisioning, personnel screening)? [CTRL:SG2.SP1],[HRM:SG3.SP1]

Question Intent: To determine if **cybersecurity human resource practices have been implemented** for the critical service.
NIST SP 800-53 Rev. 4 PS Family:
Example cybersecurity human resource practices include:

- assigning a risk designation to organizational positions
- personnel screening and rescreening processes
- personnel termination processes
- personnel transfer process
- implementing and managing access agreements (nondisclosure agreements, acceptable use agreements, access agreements, etc.)
- third-party personnel security processes
- personnel sanctions for noncompliance

Criteria for "Yes" Response:

- ***Cybersecurity human resource practices have been implemented*** *for the critical service.*

Criteria for "Incomplete" Response:

- *Cybersecurity human resource practices are* ***in development and partially implemented****.*

10. Is access to systems and assets controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting)? [CTRL:SG2.SP1],[TM:SG2.SP2]

Question Intent: To determine if **access to systems and assets** that support the critical service **is controlled, in accordance with the principle of least functionality.**
NIST SP 800-53 Rev. 4 AC-3, CM-7:

- Information systems should be **configured to provide only essential capabilities** and prohibit or restrict the use of unnecessary functions, ports, protocols, services, etc.
- Where feasible, organizations should **limit component functionality to a single function** per device/system (e.g., email server or web server but not both).
- Other examples of least functionality include:
  - allowlisting (whitelisting)
  - denylisting (blacklisting)
  - preventing program execution

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.18 Control connection of mobile devices.	CM.L2-3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM.L2-3.4.7 Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services.
CM.L2-3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software	SC.L2-3.13.3 Separate user functionality from system management functionality.	

Criteria for "Yes" Response:

- ***Access to all systems and assets*** *that support the critical service* ***is controlled in accordance with the principle of least functionality****.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements*** *listed in the guidance for this practice are* ***implemented, addressed, or considered in the context of the practice****.*

Criteria for "Incomplete" Response:

- *Access to* ***some*** *systems and assets is controlled in accordance with the principle of least functionality.*

Goal 3 – Control designs are analyzed to ensure they satisfy control objectives.

1. Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1]

Question Intent: To determine if controls **satisfy** the established **control objectives**.

- **Controls analysis establishes a baseline** from which the organization can begin to assess control effectiveness on a scheduled basis.
- **Controls analysis should identify gaps** where a control objective is not adequately satisfied.
- **Analysis** may include:
  - a **design review** of the control and its ability to meet the control objective.
  - **development** and **execution of tests** that demonstrate the control's capability.

Typical work products:

- analysis results
- control objectives that are satisfied by controls
- a traceability matrix of control objectives and the controls that satisfy them
- control gaps
- proposed updates to existing controls
- proposed new controls
- risks related to unsatisfied control objectives
- risks related to redundant and conflicting controls

Criteria for "Yes" Response:

- *The organization has* ***analyzed all the controls****.*
- *And; the organization has* ***identified gaps*** *where existing controls do not meet the control objectives.*

Criteria for "Incomplete" Response:

- ***Some*** *controls have been analyzed against control objectives.*

2. **As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]**

Question Intent: To determine if **existing controls are modified or new controls are implemented to resolve gaps.**

Criteria for "Yes" Response:

- *The organization uses the output of the controls gap analysis (CTRL:G3.Q1) to address all gaps that require resolution by:*
  - ***modifying** existing controls*
  - *Or; **introducing new** controls*

Criteria for "Incomplete" Response:

- ***Some** gaps discovered from analysis are **addressed**.*

Goal 4 – The internal control system is assessed to ensure control objectives are met.

1. **Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]**

Question Intent: To **periodically** (as defined by the organization) **determine** if established controls **continue to meet** control objectives**.**

- The assessment verifies controls **continue to protect and sustain** the critical service and **identifies any controls that do not.**
- The organization can use the analysis of control designs (established in G3.Q1) as the **baseline** of continuous assessment.
- The organization **sets the assessment schedule.**
- The organization should **consider regulatory obligations and internal policy** for performance and scheduling requirements.

Typical work products:

- assessment results
- control objectives that are satisfied by controls
- control gaps (control objectives not satisfied by controls)
- proposed updates to existing controls
- proposed new controls
- remediation plans
- updates to service continuity plans
- risks related to unsatisfied control objectives
- risks related to redundant and conflicting controls

Criteria for "Yes" Response:

- *The organization **periodically** (as defined by the organization) **assesses** the performance of all controls to ensure that they continue to meet control objectives.*

Criteria for "Incomplete" Response:

- *The organization has **not established a frequency** to assess the performance of controls.*
- *Or; **some controls are assessed** against control objectives.*

2. **As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]**

CYBER RESILIENCE ANALYSIS

Question Intent: To ensure that **problem areas** or **gaps** are **addressed** by modifying existing controls or implementing new controls. Problem areas **require remediation** to ensure that controls **continue to satisfy** control objectives**.**

Criteria for "Yes" Response:

- ***All*** *gaps have been addressed by the modification of existing controls or the implementation of new controls.*

Criteria for "Incomplete" Response:

- ***Some*** *gaps have been addressed.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing controls management activities? [CTRL:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** controls management activities **exists.**

- The plan defines controls management within the organization and **prescribes how controls management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- control management activities (control design, analysis and assessment methodology)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a* ***documented plan*** *for performing controls management.*

Criteria for "Incomplete" Response:

- *A plan is* ***in development and partially documented****.*

2. Is there a documented policy for controls management? [CTRL:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** controls management activities **exists.**

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the controls management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform controls management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing the control environment

- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing controls management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for controls management activities been identified and made aware of their roles? [CTRL:GG2:GP7]

Question Intent: To determine if **stakeholders** for controls management activities have been **identified** and **made aware of their roles.**

Stakeholders of the controls management process have the following **responsibilities**:

- defining and managing control objectives and controls, including ensuring the effectiveness of controls
- overseeing the controls management process
- managing the risk resulting from unresolved problems (gaps in controls, insufficient staffing or funding, etc.)

Examples of stakeholders include**:**

- critical service owners
- management
- controls management staff
- owners and custodians of assets that underpin the service
- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors

Criteria for "Yes" Response:

- ***All** stakeholders for the controls management activities have been **identified** and **made aware** of their roles.*

Criteria for "Incomplete" Response:

- ***Some** stakeholders for the controls management activities have been **identified** and **made aware** of their roles.*
- ***Or; stakeholders are identified but have not been made aware of their roles.***

4. Have controls management standards and guidelines been identified and implemented? [CTRL:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing controls management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **controls management activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- defining and selecting control objectives
- prioritizing control objectives
- implementing controls to meet objectives (for example, controls could be selected from the NIST 800-53 recommended security control, NERC CIP standards, and Control Objectives for Information and Related Technology [COBIT] standard).
- evaluating and acquiring tools for monitoring the performance of controls
- analyzing and assessing controls
- identifying gaps in controls and approaches for addressing them
- identifying redundant and conflicting controls
- identifying risks associated with problems in the control environment
- periodically assessing the control environment

Criteria for "Yes" Response:

- *The organization has **implemented documented standards and guidelines** for performing controls management activities.*

Criteria for "Incomplete" Response:

- ***Some** standards and guidelines have been **implemented**.*

MIL3-Managed

1. **Is there management oversight of the performance of the controls management activities? [GG2.GP8],[CTRL:GG2.GP8]**

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the controls management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the controls management activities.
- **Oversight** provides **visibility** into the controls management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products (assessment results, control designs, control objectives, documentation) or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the controls management activities
- escalating issues that require higher-level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day controls management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day control management activities.*

CYBER RESILIENCE **ANALYSIS**

2. Have qualified staff been assigned to perform controls management activities as planned? [CTRL:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan.**

- Qualified means that **staff are appropriately skilled** to perform controls management activities.

Examples of staff include personnel responsible for:

- designing, implementing, and assessing controls
- implementing processes, standards, and guidelines
- addressing issues and problems, including developing and executing remediation plans

Examples of skills needed include:

- knowledge necessary to elicit and prioritize stakeholder requirements and interpret them to develop effective control objectives
- knowledge of control objectives necessary for control design
- proficiency with tools, techniques, and methods used to design, analyze, assess, and manage controls

Criteria for "Yes" Response:

- ***All staff*** *assigned to perform the planned controls management activities are* ***appropriately skilled****.*

Criteria for "Incomplete" Response:

- ***Some staff*** *assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform controls management activities as planned? [CTRL:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided.** The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher-level management support and sponsorship of controls management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned controls management activities include**:**

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned controls management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. **Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled? [CTRL:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]**

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the controls management activities**.**

- The intent is to **determine risks that prevent the organization from performing controls management activities** (controls management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the controls management process include:

- poorly defined controls management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of **all** planned controls management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of **some** of the planned controls management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned controls management activities are **identified, but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. **Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results? [CTRL:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **controls management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement.**

Periodic (as defined by the organization) reviews of the controls management process are needed to ensure that**:**

- control objectives continue to be satisfied
- control problem areas are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risk related to control problem areas are identified and addressed
- actions requiring management involvement are elevated in a timely manner

Example metrics of the controls management process may include:

- percentage of control objectives that are fully satisfied by existing controls
- time and resources expended to conduct an analysis (baseline) or assessment (periodic) of controls
- number of problem areas resulting from assessments

Criteria for "Yes" Response:

- ***All*** *controls management activities are* ***periodically*** *(as defined by the organization)* ***reviewed*** *and* ***measured*** *and the* ***results evaluated****.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review of the controls management activities.*
- *Or; review and measurement addresses* ***some*** *of the controls management activities.*
- *Or; controls management activities are* ***reviewed but not measured****.*

2. Are controls management activities periodically reviewed to ensure they are adhering to the plan? [CTRL:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To **periodically** determine if controls management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the controls management plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing controls management activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- ***All*** *controls management activities are* ***periodically (as defined by the organization) reviewed*** *to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review.*
- *Or;* ***some*** *controls management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of controls management? [CTRL:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of controls management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the controls management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes**:**

- **status reviews** of controls management activities
- **issues** identified in process and plan reviews
- **risks** associated with controls management activities.
- **recommendations** for improvement

CYBER RESILIENCE
ANALYSIS

Criteria for "Yes" Response:

- *Higher-level management is **made aware of issues** related to the performance of controls management through **scheduled** communication.*

Criteria for "Incomplete" Response:

- *The organization has **not established a frequency** for communication to higher-level management.*
- *Or; communications address **some** issues.*

MIL5-Defined

1. **Has the organization adopted a standard definition of controls management activities from which operating units can derive practices that fit their unique operating circumstances? [CTRL:GG3.GP1],[GG3.GP1]**

Question Intent: To determine if the organization has a **standard process** that defines controls management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in controls management activities across the organization.

A **standard definition** may include**:**

- process description
- process activities and practices to be performed
- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of controls management.*

Criteria for "Incomplete" Response:

- *A standard definition of controls management is **in development and partially documented**.*

2. **Are improvements to controls management documented and shared across the organization? [CTRL:GG3.GP2],[GG3.GP2]**

Question Intent: To ensure that **improvements** to the controls management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the controls management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include**:**

- process metrics and measurements
- lessons learned from control analysis and assessments
- lessons learned from satisfying control objectives
- risk evaluations

CYBER RESILIENCE **ANALYSIS**

Criteria for "Yes" Response:

- ***Improvements*** *to controls management processes are* ***documented*** *and* ***shared*** *across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements*** *to controls management processes* ***are inconsistently documented****.*
- *Or;* ***not consistently shared*** *across the organization.*

CYBER RESILIENCE
ANALYSIS

3 Configuration and Change Management

The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits.

Goals and Practices

Goal 1 – The life cycle of assets is managed.

1. Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]

Question Intent: To determine if a **change management** process is **used to manage asset modifications**. Change management is a **continuous process** of controlling and approving changes to assets that support the service.

This process addresses:

- addition of new assets
- changes to the asset, including ownership, custodianship, and location
- elimination of assets

Typical work products:

- change requests
- change implementation plan
- backout plan
- change and configuration management board meeting minutes
- change approvals
- change tracking and status
- change documentation, including test results

Criteria for "Yes" Response:

- *A **change management process is used** to control changes to **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *A change management process is used to control changes to **some** assets.*

2. Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]

Question Intent: To determine if **resilience requirements are evaluated as a result of changes** to assets.

- The organization should **evaluate the impact** of asset changes **on existing resilience requirements.**
- **The requirements from all the services supported by the changed asset should be considered**. Evaluating resilience requirements is especially critical when assets are shared between services.

Typical work products:

- documented criteria that establishes when a change in requirements must be evaluated
- requirements change history with rationale for performing the change
- requirements baseline
- resilience requirements included in change requests
- updated asset resilience requirements

Criteria for "Yes" Response:

- *The organization **evaluates all of the resilience requirements of each asset** that supports the critical service when changes to the asset occur.*

Criteria for "Incomplete" Response:

- *The organization evaluates **some of the resilience requirements** of each asset that supports the critical service when changes to the asset occur.*
- *Or; the organization evaluates all of the resilience requirements of **some assets** when changes to the asset occur.*

3. Is capacity management and planning performed for assets? [TM:SG5.SP3]

Question Intent: To determine if **capacity management and planning is performed** for assets.

- **Capacity planning determines the operational demand** for a technology asset over a variable range of operational needs.
- Capacity management and planning involves:
  - **measurement** of current demand
  - **tests** for anticipated demand
  - and **gathering usage trends** over time to be able to predict expansion needs.

Typical work products include:

- capacity management strategy
- capacity forecasts
- capacity statistics and performance metrics

Criteria for "Yes" Response:

- *The organization **performs capacity management and planning** for **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization performs capacity management and planning for **some** assets.*

4. Are change requests tracked to closure? [TM:SG4.SP3]

Question Intent: To determine if **change requests are tracked to closure**.

- This activity ensures that all change requests have a disposition.
- And; changes that have not been closed are provided an updated status.

Typical work products:

- status reports
- change request database
- open items list

Criteria for "Yes" Response:

- ***All change requests** are tracked to closure.*

Criteria for "Incomplete" Response:

- ***Some** change requests are tracked to closure.*

5. Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]

Question Intent: To determine if **stakeholders are notified when** they are **affected by changes** to assets.

- The organization should **establish communication channels** to ensure stakeholders are aware of changes to assets.
- The organization should **update service level agreements** with stakeholders if necessary to reflect commitment to change notifications.

Criteria for "Yes" Response:

- ***Stakeholders are notified*** *of* ***all*** *changes to assets that affect them.*

Criteria for "Incomplete" Response:

- *Stakeholders are notified of* ***some*** *changes to assets that affect them.*

6. Is a System Development Life Cycle implemented to manage systems supporting the critical service? [ADM:SG3.SP2][RTSE:SG2.SP2]

Question Intent: To determine if a **System Development Life Cycle is implemented** to manage systems and assets that support the critical service.

NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8:

- **A well-defined System Development Life Cycle** provides the foundation for the successful development, implementation, operation, and disposal of organizational information systems.
- Information system **security engineering principles** (ensuring security is a design requirement, developers are trained accordingly, etc.) **are incorporated and applied to** the specification, design, development, implementation, and modification of information systems.
- **Maintaining the integrity of changes** requires configuration control throughout the System Development Life Cycle.
- **Security testing/evaluation** occurs at all post-design phases of the System Development Life Cycle.

Criteria for "Yes" Response:

- *A* ***System Development Life Cycle is implemented*** *to manage* ***all*** *systems and assets that support the critical service.*

Criteria for "Incomplete" Response:

- *A System Development Life Cycle is implemented to manage* ***some*** *systems and assets that support the critical service.*

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

1. Is configuration management performed for technology assets? [TM:SG4.SP2]

Question Intent: To determine if **configuration management** is **performed for technology assets**.

- **Configuration management is a process for managing the integrity** of a technology asset over its lifetime.
- The **resilience of critical services and technology assets** may be affected when the integrity of those assets is compromised.

Configuration management:

- **supports the integrity of technology assets** by ensuring that they can be restored to an acceptable form when necessary (perhaps after a disruption)
- **provides a level of control over changes** that can potentially disrupt the asset's support to the service

Configuration management activities can include:

- determining which assets to place under configuration management
- identifying the configuration of selected assets
- creating configuration baselines
- controlling changes to configuration items
- maintaining the integrity of baseline configurations
- auditing configuration baselines

Criteria for "Yes" Response:

- *The organization **performs configuration management** for **all** technology assets that support the service.*

Criteria for "Incomplete" Response:

- *The organization performs configuration management for **some** technology assets.*

2. Are techniques in use to detect changes to technology assets? [TM:SG4.SP3]

Question Intent: To determine if **techniques** are in use **to detect changes to technology assets**.
Techniques for detecting changes help to ensure that only an approved and tested version of a technology asset is in production.

Typical techniques include:

- audits (configuration baselines, logs, etc.)
- automated tools (security integrated event manager (SIEM), baseline configuration scanners, etc.)
- procedural methods

Criteria for "Yes" Response:

- ***Techniques are in use to detect changes** for **all** technology assets that affect the critical service.*

Criteria for "Incomplete" Response:

- *Techniques are in use to detect changes for **some** technology assets.*

3. Are modifications to technology assets reviewed? [TM:SG4.SP2; TM:SG4.SP3]

Question Intent: To determine if **modifications** to technology assets are **reviewed**.

- Proposed changes to assets are analyzed to **determine the impact** to the critical service including the resilience requirements.
- Changes are also evaluated for their **potential impact to multiple services.**

Criteria for "Yes" Response:

- ***All modifications** to technology assets that support the critical service are reviewed.*

Criteria for "Incomplete" Response:

- ***Some** modifications to technology assets are reviewed.*

4. Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1]

Question Intent: To determine if **integrity requirements of information assets** are used to **determine which staff members** are **authorized to modify** those assets.

- **Integrity requirements address qualities** to ensure the information is:
  - complete and intact
  - accurate and valid
  - authorized and official
- Controlling which staff members are authorized to modify information assets helps ensure the continued integrity of those assets.
- A fundamental way of controlling modifications to information assets is to limit access to those assets, both:
  - electronically (by controlling access to networks, servers, application systems, and databases and files)
  - physically (by limiting access to file rooms, work areas, computer rooms, and facilities)

Criteria for "Yes" Response:

- *The **integrity requirements** for **each** information asset that supports the critical service are used to **determine which staff members** are authorized to modify that asset.*

Criteria for "Incomplete" Response:

- *The **integrity requirements** for **some** information assets are used to **determine which staff members** are authorized to modify those assets.*

5. Is the integrity of information assets monitored? [KIM:SG5.SP3]

Question Intent: To determine if **the integrity of information assets** that support the critical service **is monitored**.

- The **alteration of information assets through the processing cycle of the critical service must be controlled** to ensure that the resulting information asset remains complete, accurate, and reliable.
- Alteration of information assets can be due to:
  - unauthorized access or changes
  - operational risk such as loss of power (resulting in a corrupted file or database)
  - authorized changes resulting in unintended changes to the information asset

Typical monitoring practices include:

- establishing data validation controls such as selecting records for recalculation and review
- performing regular reviews of information asset outputs from processes
- periodically verifying that changes are valid and authorized (e.g., audits)

Criteria for "Yes" Response:

- *The **integrity of all information assets** that support the critical service **is monitored**.*

Criteria for "Incomplete" Response:

- *The integrity of **some** information assets is monitored.*

6. Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2; TM:SG4.SP3]

Question Intent: To determine if **unauthorized or unexplained modifications** to technology assets **are addressed**.

- **Periodically verify** (through monitoring and auditing) that changes to configurations are valid and authorized.
- **Identify action items** that are required to repair any unauthorized or unexplained modifications to technology assets.
- **Track** action items **to closure.**

Criteria for "Yes" Response:

- ***All unauthorized or unexplained modifications*** *to technology assets that support the critical service are* ***addressed****.*

Criteria for "Incomplete" Response:

- ***Some*** *unauthorized or unexplained modifications to technology assets are addressed.*

7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]

Question Intent: To determine if **modifications to technology assets are tested** before being committed to production. The purpose is to **ensure** that only **tested and approved versions** of assets are in production.

- To minimize operational impact, the organization should **test in a segregated test environment** to identify issues.
- Once all issues have been identified and addressed, the organization can move the modified technology asset into production.

Typical work products:

- release management policy, guidelines, and standards
- test builds
- test procedures
- test results

Criteria for "Yes" Response:

- ***All modifications*** *to technology assets that support the critical service* ***are tested*** *before being committed to production.*

Criteria for "Incomplete" Response:

- ***Some*** *modifications to technology assets are tested before being committed to production.*

8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]

Question Intent: To determine if a **process for managing access** to technology assets has been implemented.

- The process should address:
  - **identifying and documenting** staff who are authorized to modify technology assets
  - access **requests and approvals**
  - **periodic auditing** of technology assets to identify unauthorized access
- **Controlling access** to technology assets by authorized staff **ensures the continued integrity** of these assets by limiting their unauthorized or inadvertent modification.
- Access controls for technology assets may take **electronic or physical forms.** For example:
  - ensuring that technology assets are protected behind a physical barrier.
  - ensuring that technology assets are protected using role-based electronic access controls.

Criteria for "Yes" Response:

- *There is a* ***documented and implemented process*** *for managing access to technology assets that support the critical service.*

Criteria for "Incomplete" Response:

- *A process for managing access to technology assets is* ***in development and partially implemented****.*

9. Is the maintenance and repair of assets performed and logged in a timely manner? [ADM:SG3.SP2],[TM:SG5.SP2]

Question Intent: To determine if the **maintenance and repair** of assets are **performed and logged in a timely manner.**

NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5:

- Organizations should **schedule, perform, document, and review records of maintenance and repairs** on information system components.
- **All maintenance activities**, whether performed on site or remotely, **should be approved and monitored.**
- A process for **authorizing maintenance personnel** and for **keeping a list** of authorized personnel or maintenance organizations should be established.

Criteria for "Yes" Response:

- *The **maintenance and repair** of **all** assets that support the critical service are performed and logged in a timely manner.*

Criteria for "Incomplete" Response:

- *The maintenance and repair of **some** assets that support the critical service are performed and logged in a timely manner.*

10. Is the maintenance and repair of assets performed with approved and controlled tools and/or methods? [ADM:SG3.SP2][TM:SG5.SP2]

Question Intent: To determine if the **maintenance and repair** of assets are **performed with approved and controlled tools and/or methods.**

NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5:

- Organizations **should approve, control, and monitor** information system **maintenance tools.**

Criteria for "Yes" Response:

- *The **maintenance and repair** of **all** assets that support the critical service are **performed with approved and controlled tools and/or methods**.*

Criteria for "Incomplete" Response:

- *The maintenance and repair of **some** assets that support the critical service are performed with approved and controlled tools and/or methods.*

11. Is the remote maintenance and repair of assets approved, logged, and performed in a manner that prevents unauthorized access? [ADM:SG3.SP2][TM:SG5.SP2]

Question Intent: To determine if the **remote maintenance and repair** of assets are **approved, logged, and performed to prevent unauthorized access.**

NIST SP 800-53 Rev. 4 MA-4:

- Organizations should:
  - **Approve and monitor** remote maintenance and diagnostic activities.
  - **Employ strong authentication** when establishing remote maintenance and diagnostic sessions.
  - **Maintain records/logs** for remote maintenance and diagnostic activities.
  - **Terminate sessions and network connections** when remote maintenance and diagnostic activities are completed.
- **Strong authentication** requires authenticators that are **resistant to replay attacks and employ multifactor authentication.**

- **Strong authenticators** can include:
  - public key infrastructure (PKI) certificates
  - passphrases
  - biometrics

Criteria for "Yes" Response:

- *The **remote maintenance and repair** of **all** assets that support the critical service **are approved, logged, and performed in a manner that prevents unauthorized access**.*

Criteria for "Incomplete" Response:

- *The remote maintenance and repair of **some** assets that support the critical service are approved, logged, and performed in a manner that prevents unauthorized access.*

Goal 3 – Asset configuration baselines are established.

1. Do technology assets have configuration baselines? [TM:SG4.SP2]

Question Intent: To determine if **configuration baselines exist** for technology assets that support the service.

- Establishing a **technology asset baseline** (commonly called a configuration item) **provides a foundation for managing the integrity of the asset** as it changes over its lifecycle.
- A configuration item **may also extend to other technology work products such as test scripts, test plans, and asset documentation.**
- A configuration item **may also be a grouping of related assets** that are tied together in a logical baseline.
- Configuration management establishes additional controls over the configuration baseline so that the **asset integrity is maintained** and always in a form that is available and authorized for use.

Example configuration items:

- software and application code
- operating systems
- hardware configuration files
- firewall rulesets
- configuration files for router and other network equipment

Criteria for "Yes" Response:

- ***Configuration baselines exist** for **all** technology assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Configuration baselines exist for **some** technology assets.*

2. Is approval obtained for proposed changes to baselines? [TM:SG4.SP3]

Question Intent: To determine if approval is obtained for changes to **configuration baselines** of the technology assets that support the critical service.

- An important component of configuration management is the ability to **control and manage changes** to the configuration baselines of technology assets.
  - Changes to technology assets will be handled in a controlled manner throughout their life cycle
- Because of the nature of the operational environment, most technology assets are expected to change over time. For example:
  - the addition of new functionality
  - repair of software bugs and security vulnerabilities

  - the retirement or replacement of hardware components
- **Defining and communicating change procedures,** including approval of proposed changes to baselines from relevant stakeholders, **ensures that changes** to technology assets will be **handled in a controlled manner.**

Criteria for "Yes" Response:

- ***Approval is obtained*** *for* ***all*** *proposed changes to configuration baselines of the technology assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Approval is obtained for* ***some*** *proposed changes to configuration baselines.*

3. Has a baseline of network operations been established? [TM:SG4.SP2]

Question Intent: To determine if a **baseline of network operations** for all systems and assets that support the critical service **has been established.**

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4:

- **Baseline configurations include** information about **information system components, network topology,** and the **logical placement of those components** within the system architecture.
- **Baseline configurations** for information systems and assets **are developed, documented,** and maintained under configuration control.

Criteria for "Yes" Response:

- *A* ***baseline of network operations has been established*** *for* ***all*** *systems and assets that support the critical service.*

Criteria for "Incomplete" Response:

- *A baseline of network operations has been established for* ***some*** *systems and assets that support the critical service.*

4. Is the baseline of network operations managed? [TM:SG4.SP2]

Question Intent: To determine if **the established baseline of network operations is managed** for all systems and assets that support the critical service.

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4:

- **Baseline configurations** for information systems and assets are developed, documented, and **maintained under configuration control.**
- Baseline configurations are **formally reviewed.**
- **Maintaining baseline configurations requires creating new baselines** as organizational information systems change over time.

Criteria for "Yes" Response:

- *The established* ***baseline of network operations is managed*** *for* ***all*** *systems and assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The established baseline of network operations is managed for* ***some*** *systems and assets.*

5. Has a baseline of expected data flows for users and systems been established? [TM:SG4.SP2]

Question Intent: To determine if a **baseline of expected data flows** for all user and system assets that support the

critical service **has been established.**

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4:

- **Information flow control regulates where information is allowed to travel** within an information system and between information systems.
- **Dedicated connections** between information systems **should be authorized.**
- The interconnection **interface characteristics, security requirements,** and the nature of the communication should be **documented** as part of the baseline.

Criteria for "Yes" Response:

- ***A baseline of expected data flows has been established*** *for* ***all*** *user and system assets that support the critical service.*

Criteria for "Incomplete" Response:

- *A baseline of expected data flows has been established for* ***some*** *user and system assets.*

6. Is the baseline of expected data flows for users and systems managed? [TM:SG4.SP2]

Question Intent: To determine if **the established baseline of expected data flows is managed.**

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4:

- **Dedicated connections should be periodically** (frequency defined by the organization) **reviewed and updated.**
- **Baseline configurations** for information systems and assets are developed, documented, and **maintained under configuration control.**
- Baseline configurations are **formally reviewed.**
- **Maintaining baseline configurations requires creating new baselines** as organizational information systems change over time.

Criteria for "Yes" Response:

- *The established* ***baseline of expected data flows*** *is managed for* ***all*** *user and system assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The established baseline of expected data flows is managed for* ***some*** *user and system assets.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing change management activities? [TM:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** change management activities **exists**.

- The plan defines change management within the organization and **prescribes how change management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- change management activities (change management process, establishing and managing baselines, capacity management, etc.)

- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing change management.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for change management? [TM:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** change management activities **exists**.

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the change management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform change management activities
- establishment of procedures, standards, and guidelines
- requesting and approving changes to assets
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing change management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for change management activities been identified and made aware of their roles? [TM:GG2:GP7]

Question Intent: To determine if **stakeholders** for change management activities have been **identified** and **made aware of their roles**.

Stakeholders of the change management process have the following **responsibilities**:

- creating asset baselines
- overseeing the change management process
- capacity management planning
- configuration management
- requesting and approving changes to assets
- resolving issues in the change management process

Examples of stakeholders include**:**

- critical service owners

- management
- change management staff
- owners and custodians of assets that underpin the service
- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors

Criteria for "Yes" Response:

- ***All*** *stakeholders for the change management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the change management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but have* ***not been made aware*** *of their roles.*

4. Have change management standards and guidelines been identified and implemented? [TM:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing change management activities **have been implemented**.

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **change management activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- documenting and maintaining asset descriptions
- documenting changes to resilience requirements for assets
- capacity management
- stakeholder notification
- configuration management including baselines
- requesting, approving, and implementing changes to assets

Criteria for "Yes" Response:

- *The organization has* ***implemented documented standards and guidelines*** *for performing change management activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented****.*

MIL3-Managed

1. Is there management oversight of the performance of the change management activities? [TM:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists**. The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the change management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the

change management activities.

- **Oversight** provides **visibility** into the change management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products (baselines, configuration items, capacity management plans, documentation)
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the change management activities
- escalating issues that require higher-level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day change management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day change management activities.*

2. Have qualified staff been assigned to perform change management activities as planned? [TM:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned**. The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan**.

- Qualified means that **staff are appropriately skilled** to perform change management activities.

Examples of staff include personnel responsible for:

- change management
- configuration management
- capacity management
- implementing processes, standards, and guidelines
- addressing issues and problems, including developing and executing remediation plans

Examples of skills needed include:

- knowledge of the service to effectively evaluate requested changes
- knowledge necessary to elicit and prioritize stakeholder requirements and interpret them to develop effective change control procedures
- proficiency with tools, techniques, and methods used for:
  - detecting changes in assets
  - configuration management
  - capacity management
  - change control
  - release management
  - monitoring and logging of modification activities

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned change management activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff*** *assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform change management activities as planned? [TM:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided**. The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher-level management support and sponsorship of change management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned change management activities include**:**

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned change management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled? [TM:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the change management activities.

- The intent is to **determine risks that prevent the organization from performing change management activities** (change management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the change management process include:

- poorly defined change management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned change management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of* ***some*** *of the planned change management activities are identified, analyzed, disposed of, monitored, and controlled.*

- *Or; risks to the performance of planned change management activities are **identified, but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. **Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results? [TM:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **change management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement**.
Periodic (as defined by the organization) reviews of the change management process are needed to ensure that:

- unauthorized changes are identified, tracked, and addressed
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to change management activities are identified and addressed
- actions requiring management involvement are elevated in a timely manner

Example metrics of the change management process may include:

- number of requested changes per asset
- number of unauthorized or unexplained changes
- number of approved but unincorporated changes
- number of times stakeholders weren't notified of approved changes
- number of times an approved change is implemented and then reversed
- percentage of technology assets that deviate from approved configuration baselines

Criteria for "Yes" Response:

- ***All** change management activities are **periodically** (as defined by the organization) **reviewed** and **measured** and the **results evaluated**.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review of the change management activities.*
- *Or; review and measurement addresses **some** of the change management activities.*
- *Or; change management activities are **reviewed but not measured**.*

2. **Are change management activities periodically reviewed to ensure they are adhering to the plan? [TM:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To **periodically** determine if change management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the change management plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing change management activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- *__All__ change management activities are __periodically (as defined by the organization) reviewed__ to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization __has not established a frequency__ for review.*
- *Or; __some__ change management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of change management? [TM:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of change management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the change management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes**:**

- status reviews of change management activities
- issues identified in process and plan reviews
- risks associated with change management activities
- recommendations for improvement

Criteria for "Yes" Response:

- *Higher-level management is __made aware of issues__ related to the performance of change management through __scheduled__ communication.*

Criteria for "Incomplete" Response:

- *The organization has __not established a frequency__ for communication to higher-level management.*
- *Or; communications address __some__ issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of change management activities from which operating units can derive practices that fit their unique operating circumstances? [TM:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines change management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in change management activities across the organization.

A **standard definition** may include**:**

- process description
- process activities and practices to be performed
- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement

- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of change management.*

Criteria for "Incomplete" Response:

- *A standard definition of change management is **in development and partially documented**.*

2. Are improvements to change management documented and shared across the organization? [TM:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the change management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the change management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include**:**

- process metrics and measurements
- lessons learned from the execution and review of change management activities
- direct feedback from stakeholders
- improvements based on executed or tested service continuity plans
- risk evaluations

Criteria for "Yes" Response:

- ***Improvements** to change management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to change management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

CYBER RESILIENCE
ANALYSIS

4 Vulnerability Management

The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.

Goals and Practices

Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.

1. Has a vulnerability analysis and resolution strategy been developed? [VAR:SG1.SP2]

Question Intent: To determine if a **vulnerability analysis and resolution strategy has been developed**.

- The **strategy for addressing vulnerability analysis and resolution should be documented,** communicated to relevant stakeholders, and **implemented.**
- The strategy may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The vulnerability analysis and resolution strategy should address:

- The scope of assets relevant to the critical service.
  - The scoping should be driven by the resilience requirements of the service and the identified assets.
- The essential activities that are required for vulnerability identification, analysis, and resolution.
- A process for organizing, categorizing, comparing, and consolidating vulnerabilities.
- Approved tools, techniques, and methods.
- A schedule for performing vulnerability activities.
- The skills and training required.
- Relevant stakeholders of the vulnerability activities and their roles.

Criteria for "Yes" Response:

- *There is a **documented strategy** for performing vulnerability analysis and resolution activities.*

Criteria for "Incomplete" Response:

- *A strategy is **in development and partially documented**.*

2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR:SG1.SP2]

Question Intent: To determine if a **standard set of tools and/or methods are in use** to identify vulnerabilities in assets.

- **Pre-approving** tools, techniques, and methods **ensures consistency**, as well as **validity of results.**
- The tools and methods should **cover all the assets that support the critical service.**
- The tools and methods can be both **procedural and automated.**
- Vulnerabilities in people assets should include looking for **unskilled or unqualified personnel** placed in skilled roles.

Criteria for "Yes" Response:

- *The organization has a **standard set of tools and/or methods** that are used to identify vulnerabilities in **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has a **standard set of tools and/or methods** that are used to identify vulnerabilities in **some** assets.*

3. Is there a standard set of tools and/or methods in use to detect malicious code in assets? [VAR:SG1.SP2]

Question Intent: To determine if a **standard set of tools and/or methods** is in use **to detect malicious code** in assets.

NIST 800-53 Rev.4 SI-3:

- The organization **employs malicious code protection mechanisms at designated information system entry and exit points** to detect and eradicate malicious code.
- **The organization updates malicious code protection mechanisms** whenever new releases are available.
- **The organization performs periodic scans** (as defined by the organization) of the information system and real-time scans of files from external sources.

Criteria for "Yes" Response:

- *The organization has a **standard set of tools and/or methods** that are used to **identify malicious code**, where appropriate, in **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has a standard set of tools and/or methods that are used to identify malicious code, where appropriate, in **some** assets.*

4. Is there a standard set of tools and/or methods in use to detect unauthorized mobile code in assets? [VAR:SG1.SP2]

Question Intent: To determine if a **standard set of tools and/or methods** is in use **to detect unauthorized mobile code** in assets.

NIST 800-53 Rev.4 SC-18, SI-4. SC-44:

- **Mobile code technologies** include:
  - Java and JavaScript
  - ActiveX
  - PDFs
  - Shockwave movies
  - Flash animations
- The organization should:
  - **define acceptable and unacceptable** mobile code technologies
  - **establish usage restrictions** and implementation guidance
  - **authorize, monitor, and control** the use of mobile code within information systems
- Corrective actions when unacceptable mobile code is detected include:
  - blocking file transmissions
  - quarantining
  - alerting administrators/security personnel

CYBER RESILIENCE **ANALYSIS**

Criteria for "Yes" Response:

- *The organization has a **standard set of tools and/or methods** that are used to **detect unauthorized mobile code**, where appropriate, in **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has a standard set of tools and/or methods that are used to detect unauthorized mobile code, where appropriate, in **some** assets.*

5. Is there a standard set of tools and/or methods in use to monitor assets for unauthorized personnel, connections, devices, and software? [VAR:SG1.SP2]

Question Intent: To determine if a **standard set of tools and/or methods** is in use **to monitor assets for unauthorized personnel, connections, devices, and software.**

NIST 800-53 Rev.4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4:

- **Enforce physical access controls to information systems** in addition to the physical access controls for facilities (badging system, guard rounds, etc.).
- **Monitor physical access to facilities where the information systems reside** to detect and respond to physical security incidents.
- **Monitor** information systems to detect **unauthorized local, network, and remote connections.**
- **Information system monitoring** capability is achieved through a variety of **tools and techniques** that may include:
  - intrusion detection systems
  - intrusion prevention systems
  - audit record monitoring software
  - network monitoring software

Organizations in the Defense Industrial Base should be cognizant of the CUI requirements contained within Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171. The CUI Requirements that should be considered when evaluating this CRA practice include:

Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirement		
AC.L2-3.1.12 **Monitor and control remote access sessions.**	**AC.L2-3.1.18** **Control connection of mobile devices.**	**CM.L2-3.4.9** **Control and monitor user-installed software.**
PE.L2-3.10.2 **Protect and monitor the physical facility and support infrastructure for organizational systems.**	**PE.L1-3.10.3** **Escort visitors and monitor visitor activity**	**SI.L1-3.14.5** **Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.**
SI.L2-3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI.L2-3.14.7 Identify unauthorized use of organizational systems.	

Criteria for "Yes" Response:

- *The organization has a **standard set of tools and/or methods** that are used to **monitor all assets** that support the critical service **for unauthorized personnel, connections, devices, and software**.*
- ***All of the Cyber Security Maturity Model Certification (CMMC) / NIST Special Publication 800-171 CUI Requirements** listed in the guidance for this practice are **implemented, addressed, or considered in the context of the practice**.*

Criteria for "Incomplete" Response:

- *The organization has a standard set of tools and/or methods that are used to monitor **some** assets for unauthorized personnel, connections, devices, and software.*

Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.

1. Have sources of vulnerability information been identified? [VAR:SG2.SP1]

Question Intent: To determine if **sources of vulnerability information** have been **identified.**

- **Internal sources** typically **provide information** about vulnerabilities that are **unique to the organization.**
- **Internal processes,** such as incident management, could be an internal source of vulnerability information.
- **External or public sources** typically provide information that is focused on common technologies.

Example sources of vulnerability information:

- vendors of software, systems, and hardware technologies
- common free catalogs, such as:
  - US-CERT Vulnerability Database
  - The Common Vulnerabilities and Exposures (CVE) List
- industry groups
- results of executing automated tools, techniques, and methods

Criteria for "Yes" Response:

- *The organization has **identified and documented sources of vulnerability information** for **all** of the assets that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has identified and documented sources of vulnerability information for **some** assets.*

2. Is the information from these sources kept current? [VAR:SG2.SP1]

Question Intent: To determine if the **vulnerability information obtained** from the established sources **is kept current.**

- Vulnerability data collection is a **continuous process.**
- The information from the sources (established in VM:G2.Q1) needs to be **continually updated.**
- New sources of vulnerability information must also be added to the source list as they emerge.

Criteria for "Yes" Response:

- *The vulnerability information from **all** of the established sources is kept current.*

Criteria for "Incomplete" Response:

- *The vulnerability information from **some** of the established sources is kept current.*

3. Are vulnerabilities being actively discovered? [VAR:SG2.SP2]

Question Intent: To determine if **vulnerabilities are actively being discovered.**

- Vulnerabilities are discovered from an **active review** of the organization's standard list of vulnerability sources.

CYBER RESILIENCE **ANALYSIS**

Techniques used to discover vulnerabilities include:

- performing internal vulnerability audits or assessments
- performing assessments of external entities
- reviewing the results of internal and external audits
- periodically reviewing vulnerability catalogs, such as the US-CERT
- reviewing notifications from identified vendor services
- reviewing notifications from identified vulnerability services
- reviewing reports from industry groups
- using reports of vulnerabilities from other processes such as the organization's service desk

Criteria for "Yes" Response:

- *Vulnerabilities are **actively being discovered** for **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Vulnerabilities are actively being discovered for **some** assets that support the critical service.*
- *Or; vulnerabilities are **inconsistently being discovered** for **all** assets that support the critical service.*

4. Are vulnerabilities categorized and prioritized? [VAR:SG2.SP3]

Question Intent: To determine if vulnerabilities are **categorized and prioritized**.

- Prioritization can be:
  - qualitative (high, medium, or low)
  - quantitative (through a numerical scale)
- Prioritization provides the organization a structured **means for determining the appropriate categorization.**

Examples of categories based on actions to be taken for vulnerability resolution:

- take no action; ignore
- fix immediately (typically the case for vendor updates or changes)
- develop and implement a vulnerability resolution strategy (typically the case when the resolution is more extensive than simple actions such as vendor updates)
- perform additional research and analysis
- refer the vulnerability to the risk management process for formal risk consideration

Typical Work Products:

- vulnerability categorization and prioritization guidelines
- list of vulnerabilities categorized and prioritized for disposition
- updated vulnerability repository

Criteria for "Yes" Response:

- *The organization **prioritizes and categorizes vulnerabilities for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization prioritizes and categorizes vulnerabilities for **some** assets.*

5. Are vulnerabilities analyzed to determine relevance to the organization? [VAR:SG2.SP3]

Question Intent: To determine if **vulnerabilities are analyzed to determine relevance** to the organization.

- Through vulnerability analysis, the organization seeks to **understand the potential threat that the vulnerability represents.**

- The organization should **assign a course of action** to each vulnerability based upon its relevance to the organization.

Vulnerability analysis includes activities to:

- understand the threat and exposure
- review trend information to determine whether the vulnerability existed before and what actions were taken to reduce or eliminate it
- identify and understand underlying causes for exposure to the vulnerability

Criteria for "Yes" Response:

- *The organization **analyzes all** vulnerabilities to determine their relevance to the critical service.*

Criteria for "Incomplete" Response:

- *The organization analyzes **some** vulnerabilities to determine their relevance to the critical service.*

6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR:SG2.SP2]

Question Intent: To determine if a **repository for recording information about vulnerabilities and their resolution is used**.

- A vulnerability repository should be used as **the central source of vulnerability lifecycle information.**
- A vulnerability repository **supports analysis, disposition, trending, root cause analysis, and vulnerability management.**

Information that should be recorded includes:

- a unique identifier
- description of the vulnerability
- date entered into the repository
- references to the source of the vulnerability
- the priority of the vulnerability (high, medium, low)
- categorization and disposition of the vulnerability
- individuals or teams assigned to analyze and remediate the vulnerability
- a log of actions taken to reduce or eliminate the vulnerability

Criteria for "Yes" Response:

- *The organization uses a repository to **record all vulnerability information** for **all of the assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization uses a repository to **record some** vulnerability information.*
- *Or; the organization uses a repository to **record all** vulnerability information for **some** assets.*

Goal 3 – Exposure to identified vulnerabilities is managed.

1. Are actions taken to manage exposure to identified vulnerabilities? [VAR:SG3.SP1]

Question Intent: To determine if **actions are taken to manage exposure** to identified vulnerabilities.

- The organization must **develop and implement a resolution strategy** to manage exposure from identified vulnerabilities.

The resolution strategy may include actions to:

- **Minimize the organization's exposure** to the vulnerability (by reducing the likelihood that the vulnerability will be exploited).
- **Eliminate the organization's exposure** to the vulnerability.

Actions taken to manage exposure may include:

- implementing software, systems, and firmware patches
- developing and implementing operational workarounds
- developing and implementing new protective controls
- updating existing controls
- developing and implementing new service continuity plans, or updating existing plans

Typical Work Products:

- vulnerability management strategies or action plans
- updated vulnerability repository, with resolution status information
- vulnerability management strategy status reports

Criteria for "Yes" Response:

- *The organization **takes action to manage exposure to all** identified vulnerabilities for **all of the assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization **takes action to manage exposure to some** identified vulnerabilities.*
- *Or; the organization **takes action to manage exposure to all** identified vulnerabilities for **some** assets.*

2. Is the effectiveness of vulnerability mitigation reviewed? [VAR:SG3.SP1]

Question Intent: To determine if the **effectiveness of vulnerability mitigation is reviewed**.

- The organization should review mitigation activities to ensure they are effective in reducing or eliminating the exposure to identified vulnerabilities.

Criteria for "Yes" Response:

- *The organization **reviews the effectiveness of all** mitigating activities.*

Criteria for "Incomplete" Response:

- *The organization reviews the effectiveness of **some** mitigating activities.*

3. Is the status of unresolved vulnerabilities monitored? [VAR:SG3.SP1]

Question Intent: To determine if the **status of unresolved vulnerabilities is monitored**.

- Unresolved vulnerabilities should be regularly monitored and reported.

Unresolved vulnerabilities are typically those whose disposition is:

- to monitor a vulnerability resolution strategy that remains incomplete
- to perform additional research and analysis
- to refer the vulnerability to the risk management process for formal risk consideration

Criteria for "Yes" Response:

- *The organization **monitors the status of all** unresolved vulnerabilities.*

Criteria for "Incomplete" Response:

- *The organization monitors the status of **some** unresolved vulnerabilities.*

Goal 4 – The root causes of vulnerabilities are addressed.

1. Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR:SG4.SP1]

CYBER RESILIENCE
ANALYSIS

Question Intent: To determine if the organization **identifies and addresses the underlying causes of vulnerabilities**.

- Root-cause analysis is a general approach for **determining the underlying causes of vulnerabilities and how to eliminate or reduce** them.

Underlying causes of vulnerabilities may include:

- poor software design
- failure of organizational policies and processes
- improper training
- operational complexity

Activities to address the root causes of identified vulnerabilities include:

- developing or improving controls
- using strategies for sustaining assets and services
- updating training and awareness activities
- correcting practices and processes that result in exposures
- developing lessons learned

Typical Work Products:

- root-cause analysis reports
- an updated vulnerability repository with analysis results

Criteria for "Yes" Response:

- *Underlying causes for vulnerabilities are identified and addressed for **all** assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Underlying causes for vulnerabilities are identified and addressed for **some** assets.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing vulnerability management activities? [VAR:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** vulnerability management activities **exists.**

- The plan defines vulnerability management within the organization and **prescribes how vulnerability management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- vulnerability management activities (source identification, vulnerability identification, prioritization, categorization, analysis, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding

- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing vulnerability management.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for vulnerability management? [VAR:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** vulnerability management activities **exists.**

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the vulnerability management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform vulnerability management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing the vulnerability management activities
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing vulnerability management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for vulnerability management activities been identified and made aware of their roles? [VAR:GG2.GP7]

Question Intent: To determine if **stakeholders** for vulnerability management activities have been **identified** and **made aware of their roles.**

Stakeholders of the vulnerability management process have the following **responsibilities**:

- overseeing the vulnerability management process
- resolving issues with the vulnerability management process
- establishing vulnerability prioritization guidelines
- assessing collected vulnerability data
- providing feedback to those responsible for providing vulnerability data
- reviewing and appraising the effectiveness of vulnerability management activities

Examples of stakeholders include:

- critical service owners
- management
- owners of external entity relationships
- vulnerability management program staff
- owners and custodians of assets that underpin the service

- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors
- acquisition and procurement staff
- enterprise risk management staff
- service continuity staff

Criteria for "Yes" Response:

- ***All*** *stakeholders for the vulnerability management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the vulnerability management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but have* ***not been made aware*** *of their roles.*

4. Have vulnerability management standards and guidelines been identified and implemented? [VAR:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing vulnerability management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance of vulnerability management activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- prioritization and categorization guidelines
- analysis and disposition
- reporting
- tool selection and use
- collection of vulnerability data

Criteria for "Yes" Response:

- *The organization* ***has implemented documented standards and guidelines*** *for performing vulnerability management activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented****.*

MIL3-Managed

1. Is there management oversight of the performance of the vulnerability management activities? [VAR:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the vulnerability management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the vulnerability management activities.
- **Oversight** provides **visibility** into the vulnerability management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the vulnerability management activities
- escalating issues that require higher-level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day vulnerability management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day vulnerability management activities.*

2. Have qualified staff been assigned to perform vulnerability management activities as planned? [VAR:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff have been assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan.**

- Qualified means that **staff are appropriately skilled** to perform vulnerability management activities.

Examples of staff include personnel responsible for:

- collecting, analyzing, and prioritizing vulnerability management requirements
- developing vulnerability management analysis and resolution plans and programs
- establishing an appropriate infrastructure for vulnerability data
- the security and protection of vulnerability data.
- manage external entities that have contractual obligations for vulnerability management analysis and resolution

Examples of skills needed include:

- knowledge of tools, techniques, and methods used to identify, analyze, remediate, monitor, and communicate vulnerabilities
- knowledge to ensure confidentiality, integrity, and availability of vulnerability data
- knowledge necessary to interpret vulnerability data and represent it to appropriate stakeholders

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned vulnerability management activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff** assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform vulnerability management activities as planned? [VAR:GG2.GP3.SP2],[GG2.GP3.SP2]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if **adequate funding** has been **provided.** The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher-level management support and sponsorship of vulnerability management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned vulnerability management activities include:

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned vulnerability management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of vulnerability management activities identified, analyzed, disposed of, monitored, and controlled? [VAR:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the vulnerability management activities**.**

- The intent is to **determine risks that prevent the organization from performing vulnerability management activities** (vulnerability management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the vulnerability management process include:

- poorly defined vulnerability management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of all planned vulnerability management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of* ***some*** *of the planned vulnerability management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned vulnerability management activities are* ***identified, but are not*** *analyzed, disposed of, monitored, or controlled.*

CYBER RESILIENCE ANALYSIS

MIL4-Measured

1. **Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results? [VAR:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **vulnerability management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement.**
Periodic (as defined by the organization) reviews of the vulnerability management process are needed to ensure that:

- vulnerability management performance issues are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to vulnerability management performance are identified and addressed
- actions requiring management involvement are elevated in a timely manner
- new vulnerabilities are identified and prioritized
- current sources of vulnerability data are in use
- vulnerability mitigation activities are effective

Example metrics of the vulnerability management process may include:

- number of reported vulnerabilities for which a vulnerability management strategy exists
- number of vulnerabilities requiring a root-cause analysis
- number of vulnerabilities referred to the risk management process
- number of vulnerabilities where corrective action is still pending

Criteria for "Yes" Response:

- ***All*** *vulnerability management activities are* ***periodically*** *(as defined by the organization)* ***reviewed*** *and* ***measured*** *and the* ***results evaluated****.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review of the vulnerability management activities.*
- *Or; review and measurement address* ***some*** *of the vulnerability management activities.*
- *Or; vulnerability management activities are* ***reviewed but not measured****.*

2. **Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan? [VAR:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To **periodically** determine if vulnerability management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the vulnerability management plan are needed to **ensure that:**

- activities are performed as planned and adhere to process descriptions, standards, and procedures
- deviations from the plan are identified and evaluated
- problems in the plan for performing vulnerability management activities are identified
- non-compliance is addressed
- needed process changes are identified when expected results or outputs are not met

Criteria for "Yes" Response:

- ***All*** *vulnerability management activities are* ***periodically (as defined by the organization) reviewed*** *to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review.*
- *Or;* ***some*** *vulnerability management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to vulnerability management? [VAR:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of vulnerability management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the vulnerability management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes:

- **status reviews** of vulnerability management activities
- **issues** identified in process and plan reviews
- **risks** associated with vulnerability management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is* ***made aware of issues*** *related to the performance of vulnerability management through* ***scheduled*** *communication.*

Criteria for "Incomplete" Response:

- *The organization has* ***not established a frequency*** *for communication to higher-level management.*
- *Or; communications address* ***some*** *issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of the vulnerability management activities from which operating units can derive practices that fit their unique operating circumstances? [VAR:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines vulnerability management activities.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in vulnerability management activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed

- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of vulnerability management.*

Criteria for "Incomplete" Response:

- *A standard definition of vulnerability management is **in development and partially documented**.*

2. Are improvements to vulnerability management documented and shared across the organization? [VAR:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the vulnerability management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the vulnerability management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include:

- process metrics and measurements
- reports on the effectiveness of controls in mitigating vulnerabilities
- lessons learned from root-cause analysis
- improvements based on risk identification and mitigation
- changes in operating conditions, risk conditions, and the risk environment that impact vulnerability management

Criteria for "Yes" Response:

- ***Improvements** to vulnerability management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to vulnerability management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

5 Incident Management

The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response.

Goals and Practices

Goal 1 – A process for identifying, analyzing, responding to, and learning from incidents is established.

1. Does the organization have a plan for managing incidents? [IMC:SG1.SP1]

Question Intent: To determine if the organization has a **documented plan for managing incidents**.

- The organization's plan for managing incidents should **address the identification, analysis, and response** to an incident.
- An **event is one or more occurrences that affect organizational assets** and have the potential to disrupt operations.
- An **incident significantly impacts** the critical service and **requires the organization to respond** to prevent or limit impact to the critical service and the organization.
- An **incident may result from an event or a series of events that requires a response** that is beyond standard operating procedures for managing events.

The organization must plan for how it will:

- identify events and incidents
- analyze these events and incidents and determine an appropriate response
- develop declaration criteria
- respond to incidents
- communicate incident information to stakeholders
- staff the plan to meet plan objectives
- structure the incident management staff (including roles and responsibilities)
- train staff to identify, analyze, and respond to incidents

Criteria for "Yes" Response:

- *There is a **documented plan** for managing incidents relevant to the critical service.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]

Question Intent: To determine if the **incident management plan is reviewed and updated.**

- The incident management plan should be **periodically (as defined by the organization) reviewed** and updated.
- The **knowledge gained through managing incidents** can be used by the organization to **improve the plan.**

Criteria for "Yes" Response:

- *The organization **periodically (as defined by the organization) reviews and updates the incident management plan**.*

Criteria for "Incomplete" Response:

- *The organization **has reviewed and updated the plan**, but **has not established a frequency** for the review.*

3. Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]

Question Intent: To determine if the **roles and responsibilities** defined in the incident management plan are **included in job descriptions**.

- The organization should **define the roles and responsibilities** to achieve the plan's objectives.
- Job descriptions are a means **to ensure that incident management staff understand** their **roles** and are **aware** of their **responsibilities.**
- Those roles and responsibilities should be **included in the job description.**

Criteria for "Yes" Response:

- ***All defined roles and responsibilities** in the incident management plan are **included in job descriptions**.*

Criteria for "Incomplete" Response:

- ***Some** defined roles and responsibilities are included in job descriptions.*

4. Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]

Question Intent: To determine if **staff have been assigned to the roles and responsibilities** detailed in the incident management plan.

- The organization should **establish a list of skilled staff and alternates** to fill each role and responsibility defined in the incident management plan.
- The organization should **assign staff** to each role and responsibility defined in the plan.

Examples of incident management skills include:

- event detection and reporting
- analyzing events and incidents
- collecting and preserving evidence

Criteria for "Yes" Response:

- ***Staff** have been **assigned to all defined roles and responsibilities** in the incident management plan.*

Criteria for "Incomplete" Response:

- *Staff have been assigned to **some** defined roles and responsibilities.*

Goal 2 – A process for detecting, reporting, triaging, and analyzing events is established.

1. Are events detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)? [IMC:SG2.SP1]

Question Intent: To determine if **events are detected and reported**.

- An **event is one or more occurrences that affect assets** and has the potential to **disrupt the critical service.**
- **Events should be captured and analyzed** to determine if the event will become (or has become) an incident that requires action.

Examples of event detection and reporting include:

- monitoring of the technical infrastructure, including information, network traffic, servers, control systems, etc.
- service desk ticketing and reporting
- monitoring of personnel
- reporting from law enforcement or legal staff
- observation of breakdowns in processes or productivity of assets
- external notification from other entities such as US-CERT
- results of audits or assessments

Criteria for "Yes" Response:

- ***Events are detected and reported*** *for* ***all*** *assets that support the critical service.*

Criteria for "Incomplete" Response:

- *Events are detected and reported for* ***some*** *assets.*

2. Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]

Question Intent: To determine if **event data is logged in an incident knowledgebase** or similar mechanism**.**

- Logging and tracking event data in an incident knowledgebase or similar mechanism:
  - **facilitates event triage and analysis** activities
  - provides the **ability to obtain a status and disposition** of the event

An incident knowledgebase should contain basic event (and incident) information such as:

- a unique identifier
- a brief description of the event
- an event category (e.g., denial of service, virus intrusion, physical access violation)
- the assets, services, and organizational units that are affected by the event
- a brief description of how the event was identified and reported, by whom, and other relevant details (e.g., application system, network segment, operating system)
- the individuals or teams to whom the event (or incident) was assigned
- relevant dates
- the actions taken and the resolution of the event

Criteria for "Yes" Response:

- *The organization* ***logs all event data*** *relevant to the critical service in an incident knowledgebase or similar mechanism.*

Criteria for "Incomplete" Response:

- *The organization logs relevant data on* ***some*** *events.*

3. Are events categorized? [IMC:SG2.SP4]

Question Intent: To determine if **events are categorized**.

- Event categories can help the organization understand and communicate the severity and impact the event will have on the critical service.
- Events may be categorized by:
  - **type** (e.g., security, safety, unauthorized access, user issue, denial of service, virus intrusion, physical access violation)
  - **severity** (e.g., critical, high, medium, low)
  - other categorization labels (e.g., internal, external, physical, technical)

Criteria for "Yes" Response:

- *The organization **categorizes all events** relevant to the critical service.*

Criteria for "Incomplete" Response:

- *The organization categorizes **some** events.*

4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]

Question Intent: To determine if **events are analyzed for their relationship to other events.**

- Analysis should be conducted to determine whether the event correlates to other events (correlation may indicate larger issues, problems, or incidents).

Criteria for "Yes" Response:

- *The organization **analyzes all events** relevant to the critical service to determine if they are related to other events.*

Criteria for "Incomplete" Response:

- *The organization **analyzes some events**.*

5. Are events prioritized? [IMC:SG2.SP4]

Question Intent: To determine if **events are prioritized.**

- Prioritization determines what order events should be addressed.
- Events may be **prioritized based on:**
  - the results of categorization (severity, type, etc.) and analysis
  - experience with past events
  - potential impact

Criteria for "Yes" Response:

- *The organization **prioritizes all events** relevant to the critical service.*

Criteria for "Incomplete" Response:

- *The organization prioritizes **some** events.*

6. Is the status of events tracked? [IMC:SG2.SP4]

Question Intent: To determine if the **status of events are tracked.**

- The **status** of events should be **checked regularly** to ensure that they are moving through the organization's established incident management process.

Possible status types for event reports include:

- closed
- referred for further analysis
- referred to an organizational unit or line of business for disposition
- declared as an incident

Criteria for "Yes" Response:

- *The organization **tracks the status of all events** relevant to the critical service.*

Criteria for "Incomplete" Response:

- *The organization tracks the status of **some** events.*

7. Are events managed to resolution? [IMC:SG2.SP4]

Question Intent: To determine if **events are managed to resolution**.

- **Periodically** (as defined by the organization) **review** the incident knowledgebase for events that have not been closed or for which there is no disposition.
- Events that have not been closed or **that do not have a disposition should be reprioritized, analyzed, and tracked to resolution.**

Criteria for "Yes" Response:

- *The organization **manages to resolution, all events** that are relevant to the critical service.*

Criteria for "Incomplete" Response:

- *The organization manages **some** events to a resolution.*

8. Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]

Question Intent: To determine if requirements **for identifying event evidence** for forensic purposes **have been identified**.

- An event may become an organizational incident that has the potential to be a violation of local, state, or federal rules, laws, and regulations. For example:
  - Securities and Exchange Commission regulatory requirements
  - state privacy laws
  - Food and Drug Administration regulatory requirements
  - chain of custody requirements
- This is often not known early in the investigation of an event, so the organization should **ensure that all event evidence is handled properly.**

Criteria for "Yes" Response:

- *The organization has **identified and documented relevant requirements** for identifying event evidence for forensic purposes.*

Criteria for "Incomplete" Response:

- *Requirements for identifying event evidence are **in development and partially documented.***

9. Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]

Question Intent: To determine if the organization has **implemented a process to ensure event evidence is handled as required** by law or other obligations.

- Based on applicable requirements (identified in IM:G2.Q8), the organization should **develop a process using standards and guidelines for the collection, documentation, and preservation of event evidence.**
- **Staff should be trained** on the organizational process for proper identification and handling of evidence to ensure that the evidence is not altered and the integrity is maintained.

Criteria for "Yes" Response:

- *There is a **documented process** to ensure event evidence is handled as required by law or other obligations.*

Criteria for "Incomplete" Response:

- *A process is **in development and partially documented**.*

CYBER RESILIENCE ANALYSIS

Goal 3 – Incidents are declared and analyzed.

1. Are incidents declared? [IMC:SG3.SP1]

Question Intent: To determine if **incidents are declared**.

- **Incident declaration defines the point** at which the organization has established that **an incident has occurred, is occurring, or is imminent.**
- Incident **declaration may occur** based **on a specific event** or when **multiple events** are occurring.

Criteria for "Yes" Response:

- *The organization **declares all incidents** relevant to the critical service.*

Criteria for "Incomplete" Response:

- *The organization declares **some** incidents.*

2. Have criteria for the declaration of an incident been established? [IMC.SG3.SP1]

Question Intent: To determine if **criteria for the declaration of incidents are established**.

- **Declaration criteria guides the organization in determining when to declare an incident** (particularly if incident declaration is not immediately apparent).

Example incident declaration criteria:

- Is the event isolated?
- Predefined thresholds of impact.
- Did past occurrences of the event result in an incident declaration?
- Is the impact of the event imminent or immediate?
- Is the organization already suffering some effects from the event?
- Is the life or safety of people at risk?
- Is the integrity and operability of a facility at risk?
- Is the integrity and operability of a high-value service or system at risk?
- Does the event constitute fraud or theft?
- Are there impacts, such as damage to the organization's reputation?
- Is there a potential legal infraction?

Criteria for "Yes" Response:

- *The organization has a **documented list of criteria** for the declaration of incidents.*

Criteria for "Incomplete" Response:

- *A documented list of criteria is **in development and partially documented**.*

3. Are incidents analyzed to determine a response? [IMC:SG3.SP2]

Question Intent: To determine if **incidents are analyzed to determine a response**.

- **Incident analysis** should focus on **properly defining the underlying problem, condition, or issue.**
- Incident analysis should help the organization **prepare the most appropriate and timely response** to the incident.
- Incident analysis should **determine** whether the incident has **legal ramifications.**

Example incident analysis activities:

- interviews with those who reported the underlying event(s) and were affected

- interviews of specific knowledge experts
- review of relevant logs and audit trails of network and physical activity
- consultation of vulnerability and incident databases (US-CERT Vulnerability Notes Database / MITRE's Common Vulnerabilities and Exposures List)
- consultation with law enforcement, legal, audit, product vendors, and emergency management

Typical work products:

- incident analysis report
- reports from analysis tools and techniques
- updated incident knowledgebase

Criteria for "Yes" Response:

- *The organization **analyzes all incidents**, relevant to the critical service, to determine a response.*

Criteria for "Incomplete" Response:

- *The organization analyzes **some** incidents to determine a response.*

Goal 4 – A process for responding to and recovering from incidents is established.

1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]

Question Intent: To determine if **incidents are escalated to stakeholders for input and resolution**.

- **Incidents** that the organization has declared **should be escalated to stakeholders** who can implement, manage, and resolve the incident.
- **Stakeholders can be internal** to the organization (such as a standing incident response team or an incident-specific team) **or external**, in the form of contractors or other suppliers.

Criteria for "Yes" Response:

- *The organization **escalates all incidents**, relevant to the critical service, **to the proper stakeholders** for input and resolution.*

Criteria for "Incomplete" Response:

- *The organization escalates **some** incidents to the proper stakeholders.*

2. Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]

Question Intent: To determine if **responses to declared incidents are developed and implemented according to pre-defined procedures**.

- The organization's **response to an incident** should be founded on **pre-defined incident response procedures.**
- Pre-defined procedures **describe the actions the organization takes to prevent or contain the impact** of an incident.
- **Incident response may be** as **simple** as notifying users to avoid opening a specific type of email message **or** as **complicated** as having to implement service continuity plans.

The actions related to incident response can include:

- containing damage (i.e., taking hardware or systems offline or by locking-down a facility)
- collecting evidence (including logs and audit trails)
- interviewing relevant staff
- communicating to stakeholders

- developing and implementing corrective actions and controls
- implementing continuity and restoration plans or other emergency actions

Criteria for "Yes" Response:

- *The organization **uses predefined procedures to develop and implement a response** to **all** declared incidents.*

Criteria for "Incomplete" Response:

- *The organization used predefined procedures to develop and implement a response to **some** declared incidents*
- *Or; pre-defined procedures for responding to declared incidents are **in development and partially documented**.*

3. Are incident status and response communicated to affected parties (including public relations staff and external media outlets)? [IMC:SG4.SP3]

Question Intent: To determine if **incident status and response are communicated** to affected parties.

- Incident status and response should be communicated **in a controlled and regular manner** to internal and external stakeholders.
- Incident status and response should be **managed throughout the incident lifecycle.**

The incident communication process should include:

- the stakeholders with whom communication about incidents are required
- the level of communication appropriate to various stakeholders
- special controls over communication (i.e., encryption or secured communications) that are appropriate for some stakeholders
- the frequency and timing of communication

Examples of stakeholders that may need to be included in incident communication:

- internal staff who have incident handling and management responsibilities
- asset owners and service owners
- information technology staff
- business continuity staff
- affected customers or suppliers
- local, state, and federal emergency management staff
- support functions such as legal, audit, and human resources
- legal and law enforcement staff (including federal agencies), if the incident may have legal ramifications
- external media outlets
- regulatory and governing agencies
- local utilities (power, gas, telecommunications, water, etc.)

Criteria for "Yes" Response:

- *The organization **communicates incident status** and response to **all affected parties**.*

Criteria for "Incomplete" Response:

- *The organization communicates incident status and response to **some** affected parties.*

4. Are incidents tracked to resolution? [IMC:SG4.SP4]

Question Intent: To determine if **incidents are tracked to resolution**.

- The organization should have a **process for the formal closure of incidents** that results in formally logging a status of closed in the incident knowledgebase.

- The **status of incidents** in the incident knowledgebase should be **reviewed regularly** to determine if open incidents should be closed or need additional action.

Typical work products:

- criteria for incident closure
- updated incident knowledgebase

Criteria for "Yes" Response:

- *The organization **tracks all incidents** relevant to the critical service **to resolution**.*

Criteria for "Incomplete" Response:

- *The organization tracks **some** incidents to resolution.*

Goal 5 – Post-incident lessons learned are translated into improvement strategies.

1. Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]

Question Intent: To determine if **analysis is performed to determine the root causes of incidents**.

- The organization should **employ commonly available techniques to perform root cause analysis** as a means of potentially preventing future incidents of a similar type and impact.

Criteria for "Yes" Response:

- *The organization **analyzes all incidents** relevant to the critical service **to determine the root cause**.*

Criteria for "Incomplete" Response:

- *The organization analyzes **some** incidents to determine the root cause.*

2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]

Question Intent: To determine if **a link between the incident management process and other related processes is established**.

- **Problem management** is the process that an organization uses to **identify recurring problems, examine root causes, and develop solutions for these problems** to prevent future, similar incidents.
- **Formal linkages to other processes** (risk management, change and configuration management, vulnerability management, etc.) that may impact an incident **should be established.**
- **Formal linkages strengthen** the organization's overall **ability to prevent incidents.**

Criteria for "Yes" Response:

- *The organization has **established a formal link** between the incident management process and other related process areas.*

Criteria for "Incomplete" Response:

- *The establishment of formal links is **in development**.*

3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]

Question Intent: To determine if **lessons learned from the incident management process are used to improve** asset protection and service continuity strategies.

- Lessons learned in incident management should help **determine the validity and effectiveness of the organization's current strategies** for protecting and sustaining assets.

- **Lessons learned should also provide** valuable information for **continuous improvement** of the incident management process.

Examples of improvements to asset protection and service continuity strategies may include:

- updated asset protection requirements
- updated controls to protect assets and services from future incidents of a similar type and nature
- updated policies to reflect lessons learned
- updated training for employees regarding the incident
- revised service continuity plans and strategies
- revised incident criteria
- standardized responses to common incidents

Criteria for "Yes" Response:

- *The organization **uses lessons learned from all incidents**, relevant to the critical service, to improve asset protection and service continuity strategies.*

Criteria for "Incomplete" Response:

- *The organization **uses lessons learned from some relevant incidents** to improve asset protection and service continuity strategies.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing incident management activities? [IMC:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** incident management activities **exists.**

- The plan defines incident management within the organization and **prescribes how incident management activities will be performed.**
- The plan may be a standalone document, embedded in a more comprehensive document, or distributed across multiple documents.

The plan typically includes:

- incident management activities (event detection, incident declaration, incident analysis, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing incident management.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for incident management? [IMC:GG2:GP1.SP2],[GG2:GP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if a **policy for performing** incident management activities **exists**.

- A **policy** is a written communication from the organization's senior management to its employees.
- It **establishes the organizational expectations** for planning and performing the incident management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform incident management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing incident management activities
- post-incident review, problem resolution, and closure
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing incident management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for incident management activities been identified and made aware of their roles? [IMC:GG2.GP7]

Question Intent: To determine if **stakeholders** for incident management activities have been **identified** and **made aware of their roles**.

Stakeholders of the incident management process have the following **responsibilities**:

- overseeing the incident management process
- making critical decisions during the incident management process
- resolving issues with the incident management process
- detecting events and incidents
- planning for incident handling, management, and response
- collecting, documenting, and preserving event and incident evidence
- analyzing events and incidents
- declaring incidents

Examples of stakeholders include:

- critical service owners and staff
- management
- incident manages
- incident owners
- staff who serve key roles in incident communication activities, such as public relations
- owners and custodians of assets that underpin the service
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors
- acquisition and procurement staff
- service continuity staff

Criteria for "Yes" Response:

- ***All*** *stakeholders for the incident management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the incident management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but* ***have not been made aware*** *of their roles.*

4. Have incident management standards and guidelines been identified and implemented? [IMC:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing incident management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **incident management activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- detecting, logging, reporting, and tracking events
- collecting and preserving evidence
- triaging events
- analyzing events
- declaring an incident from one or more events
- responding to incidents, including escalation procedures
- incident communication protocols
- creating and maintaining the incident knowledgebase

Criteria for "Yes" Response:

- *The organization has* ***implemented documented standards and guidelines*** *for performing incident management activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented****.*

MIL3-Managed

1. Is there management oversight of the performance of the incident management activities? [IMC:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the incident management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the incident management activities.
- **Oversight** provides **visibility** into the incident management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the incident management activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day incident management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day incident management activities.*

2. Have qualified staff been assigned to perform incident management activities as planned? [IMC:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff have been assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan**.

- Qualified means that **staff are appropriately skilled** to perform incident management activities.

Examples of staff include personnel responsible for:

- detecting, logging, analyzing, reporting, and tracking events
- collecting and preserving evidence
- declaring an incident from one or more events
- managing incidents and making critical decisions
- analyzing and responding to incidents, including escalation procedures
- communicating incidents
- performing post-incident reviews, resolving problems, and closing incidents
- creating and maintaining the incident knowledgebase
- managing external entities that have contractual obligations for process activities

Examples of skills needed include:

- event detection, reporting, and tracking, including service desk activities
- documenting and logging event reports
- collecting and preserving evidence
- declaring incidents
- incident analysis
- escalating and communicating incidents
- understanding and applying laws, rules, and regulations
- performing root-cause analysis and post-incident review

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned incident management activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff** assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform incident management activities as planned? [IMC:GG2.GP3.SP2],[GG2.GP3.SP2]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if **adequate funding** has been **provided**. The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of incident management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned incident management activities include:

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned incident management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of incident management activities identified, analyzed, disposed of, monitored, and controlled? [IMC:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of incident management activities.

- The intent is to **determine risks that prevent the organization from performing incident management activities** (incident management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the incident management process include:

- poorly defined incident management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned incident management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of* ***some*** *of the planned incident management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned incident management activities are* ***identified, but are not*** *analyzed, disposed of, monitored, or controlled.*

CYBER RESILIENCE ANALYSIS

MIL4-Measured

1. **Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results? [IMC:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **incident management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement.**

Periodic (as defined by the organization) reviews of the incident management process are needed to ensure that:

- incident management performance issues are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to incident management performance are identified and addressed
- actions requiring management involvement are elevated in a timely manner
- events and incidents are identified, reported, and addressed in a timely manner
- events and incidents are logged and closed
- incidents are properly declared
- post-incident reviews are performed to improve the process

Example metrics of the incident management process may include:

- number of work products that don't meet standards
- number of incidents that did not undergo post-incident review
- number of open incident management process performance issues
- percentage of incidents that are the result of exploited vulnerabilities with known solutions or patches
- percentage of incidents that require escalation
- number of events or incidents that have been logged but not closed

Criteria for "Yes" Response:

- ***All*** *incident management activities are* ***periodically*** *(as defined by the organization)* ***reviewed*** *and* ***measured*** *and the* ***results evaluated****.*

Criteria for "Incomplete" Response:

- *The organization has* ***not established a frequency*** *for review of the incident management activities.*
- *Or; review and measurement address* ***some*** *of the incident management activities.*
- *Or; incident management activities are* ***reviewed but not measured****.*

2. **Are incident management activities periodically reviewed to ensure they are adhering to the plan? [IMC:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To **periodically** determine if incident management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the incident management plan are needed to **ensure that:**

- activities are **performed as planned and adhere to process descriptions, standards, and procedures**
- deviations from the plan are identified and evaluated
- problems in the plan for performing incident management activities are identified
- non-compliance is addressed
- needed process changes are identified when expected results or outputs are not met

Criteria for "Yes" Response:

- *__All__ incident management activities are __periodically (as defined by the organization) reviewed__ to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization __has not established a frequency__ for review.*
- *Or; __some__ incident management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to incident management? [IMC:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of incident management is **communicated** to higher level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the incident management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes:

- **status reviews** of incident management activities
- **issues** identified in process and plan reviews
- **risks** associated with incident management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is __made aware of issues__ related to the performance of incident management through __scheduled__ communication.*

Criteria for "Incomplete" Response:

- *The organization has __not established a frequency__ for communication to higher-level management.*
- *Or; communications address __some__ issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of the incident management activities from which operating units can derive practices that fit their unique operating circumstances? [IMC:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines incident management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in incident management activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed
- process flow, including diagrams

- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of incident management.*

Criteria for "Incomplete" Response:

- *A standard definition of incident management is **in development and partially documented**.*

2. Are improvements to incident management documented and shared across the organization? [IMC:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the incident management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the incident management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include**:**

- process metrics and measurements
- lessons learned in the post-incident review
- improvements based on risk identification and mitigation
- recommended updates to the incident management plan

Criteria for "Yes" Response:

- ***Improvements** to incident management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to incident management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

CYBER RESILIENCE
ANALYSIS

6 Service Continuity Management

The purpose of Service Continuity Management is 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 disruptive event.

Goals and Practices

Goal 1 – Service continuity plans for high-value services are developed.

1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]

Question Intent: To determine if **service continuity plans are developed and documented** for assets required for the delivery of the critical service.

- A service continuity plan is a **proactive plan of action** an organization will take if a service disruption occurs.
- Plans should be **developed at the time of service development and implementation.**
- Plans should also be **adjusted on an ongoing basis** as new risks are encountered and the operational environment changes.
- Service continuity plans **may require one or more sub plans** such as a recovery or restoration plan.

Typical work products include:

- service continuity plan templates
- service continuity plans (including a list of relevant stakeholders)

Criteria for "Yes" Response:

- *The organization has **developed and documented service continuity plans** for **all** assets required for the delivery of the critical service.*

Criteria for "Incomplete" Response:

- *Service continuity plans have been **developed and documented for some assets**.*
- *Or; service continuity plans are **in development and partially documented**.*

2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]

Question Intent: To determine if **service continuity plans** for the critical service **are developed using standards, guidelines, and templates**.

- Standards and guidelines **ensure enterprise-wide consistency** of service continuity plans.
- Standards, guidelines, and templates can be **derived by** the organization from both **internal and external sources.**

Standards, guidelines, and templates may cover topics such as:

- alternative resources and locations that would support the organization's high-value services
- alternative activities that would have to be performed (technical or manual)
- identification of:
  - vital staff roles and responsibilities

  - high-value technology, information, and facility assets necessary to support the plan
  - relevant stakeholders of the plan and method of communicating with them
- documentation of:
  - the recovery and restoration sequence for the critical service
  - security and access-related issues that are required to execute the plan
  - any special handling that is required of information or technology
  - the service continuity test plan
  - the service continuity training plan
- coordination activities with other internal staff and external entities
- the levels of authority and access needed by responders to carry out the plan

Criteria for "Yes" Response:

- *The organization has **developed each service continuity plan** for the critical service using **established standards, guidelines, and templates**.*

Criteria for "Incomplete" Response:

- ***Some** service continuity plans are developed using standards, guidelines, and templates.*

3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]

Question Intent: To determine if **staff members are assigned to execute specific service continuity plans**.

- The **activities** documented in the service continuity plan **must be assigned** to responsible and skilled individuals in the event that the plan must be executed.
- These **staff members may be internal or external** (through outsourcing arrangements and service contracts) to the organization.

Typical work products include:

- service continuity plan staff requirements
- list of potential staff members
- staff and task assignments (internal and external)
- staff commitments to service continuity plans

Criteria for "Yes" Response:

- *The organization has **assigned staff** required for the execution of **each** service continuity plan established for the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **assigned staff** required for the execution of **some** plans.*

4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]

Question Intent: To determine if **key contacts are identified** in service continuity plans.

- The critical service may **depend on assets both internal and external to the organization.**
- Services may also rely on **external partnerships** such as public agencies and infrastructure providers (public utilities, telecommunications, etc.).
- **Key contacts** can therefore be **internal or external** to the organization.

Typical work products include:

- list of public service providers on which the critical service is dependent
- list of external entities, including business partners and vendors, that facilitate critical service delivery
- list of key contacts (both internal and external)

Criteria for "Yes" Response:

- *The organization has **identified key contacts** in **each** service continuity plan established for the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **identified key contacts** in **some** of the service continuity plans.*
- *Or; the organization has **identified some key contacts** in the service continuity plans.*

5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]

Question Intent: To determine if **service continuity plans are stored in a controlled manner and available** to those who need to know.

- The **ability to execute service continuity plans** during a disruption **depends on their accessibility and integrity.**
- The organization must take steps to ensure that the plans are:
  - archived in a controlled manner
  - up to date and available
  - secured and free from unapproved modification
  - readily retrievable, when necessary, by those who need access to them

Criteria for "Yes" Response:

- *The organization **stores all service continuity plans** for the critical service **in a controlled manner**, and the plans are **available** to **all** who need to know.*

Criteria for "Incomplete" Response:

- *The organization stores all service continuity plans for the critical service in a controlled manner, and the plans **are available to some** who need to know.*
- *Or; the organization **stores some service continuity plans** for the critical service in a controlled manner, and those plans are available to all who need to know.*

6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]

Question Intent: To determine if **availability requirements are established** for service continuity plans.

- **Availability requirements must be met by an asset** not only in day-to-day operations but also under diminished conditions brought on by a disruption or event.
- **Recovery time objectives** establish the period of acceptable downtime or the maximum time allowed for the recovery of a critical service following a disruption.
- **Recovery point objectives** establish the maximum amount of data that may be lost when service is restored after a disruption. The recovery point objective is typically expressed as a length of time. (e.g., a maximum of 4 hours' worth of data).

Criteria for "Yes" Response:

- *The organization has **established and documented availability requirements** for the critical service.*

Criteria for "Incomplete" Response:

- *Availability requirements are **in development and partially documented**.*

7. Are mechanisms (e.g., failsafe, load balancing, hot swap capabilities) implemented to achieve resilience requirements in normal and adverse situations? [TM:SG5.SP1]

Question Intent: To determine if **mechanisms are implemented to achieve resilience requirements** in normal and adverse situations.

NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6, SI-17

NIST 800-160:

The organization must plan to sustain technology assets to ensure the continued operation of services.

Mechanisms implemented to achieve this practice can take many forms:

- **load balancing:** a method that improves the distribution of workloads across multiple resources to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource
- **hot swap capabilities:** the ability to replace or add components without stopping or shutting down the associated system
- **high availability implementations:** a failover methodology to ensure availability during device or component interruptions
- alternate telecommunications services
- alternate processing sites
- fail-safe procedures:
  - fail-safe: a design feature or practice that, in the event of a specific type of failure, inherently responds in a way that will cause no or minimal harm to system assets, property, or life
  - Fail-safe procedures may include alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel).

Criteria for "Yes" Response:

- ***Mechanisms are implemented** to achieve resilience requirements for normal and adverse situations, where appropriate, **for all assets** that support the critical service.*

Criteria for "Incomplete" Response:

- ***Mechanisms are implemented** to achieve resilience requirements for normal and adverse situations, where appropriate, **for some assets**.*

Goal 2 – Service continuity plans are reviewed to resolve conflicts between plans.

1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]

Question Intent: To determine if **plans are reviewed to identify and resolve conflicts**.

- **Service continuity plans often overlap** and rely on the same set of organizational resources. For example:
  - An offsite facility that is named in more than one plan may not be able to satisfy requirements if multiple plans are executed simultaneously.
  - Multiple service continuity plans, which may need to be executed simultaneously, often rely on the same people.

Possible actions:

- Revise or rewrite conflicting plans.
- Prioritize plans to account for assets that support multiple services.
- Provide training for staff members who would be affected by plan conflicts.

Typical work products include:

- list of plan conflicts
- plan updates and remediation actions

Criteria for "Yes" Response:

- *The organization **reviews all** service continuity plans that support the critical service **to identify and resolve conflicts**.*

Criteria for "Incomplete" Response:

- *The organization **reviews some** service continuity plans to identify and resolve conflicts.*

Goal 3 – Service continuity plans are tested to ensure they meet their stated objectives.

1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]

Question Intent: To determine if **standards for testing service continuity plans have been implemented**.

- Test standards help **ensure service continuity plans are viable.**
- Testing should be **conducted in a controlled environment.**
- Testing is **often the only opportunity** for an organization to know whether the plans meet their stated objectives.
- The testing program and standards should be enforced to **ensure consistency** and the ability to interpret results at the organizational level.

Standards for service continuity testing can include:

- types of tests (i.e., walkthroughs, tabletops, dependency testing, etc.)
- required test components
- testing frequency
- quality assurance standards
- involvement and commitment of plan stakeholders
- reporting standards
- measurement standards
- test plan maintenance

Typical work products include:

- plan test program
- plan test standards

Criteria for "Yes" Response:

- *There are **documented standards** for testing service continuity plans.*

Criteria for "Incomplete" Response:

- *Standards for testing service continuity plans are **in development and partially documented**.*

2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]

Question Intent: To determine if a **schedule for testing service continuity plans is established.**

- The service continuity test **schedule should meet the requirements** of the service.

Typical work products include:

- plan test schedule

Criteria for "Yes" Response:

- *There is a **documented schedule** for testing **all** service continuity plans that support the critical service.*

Criteria for "Incomplete" Response:

- *The schedule for testing service continuity plans is **in development and partially documented**.*

3. Are service continuity plans tested? [SC:SG5.SP3]

Question Intent: To determine if **service continuity plans are tested**.

- The tests should **establish the viability, accuracy, and completeness of the plan.**
- The tests should also **provide information about the organization's level of preparedness.**
- The tests are performed under conditions established by the organization, and the **results of the test should be recorded and documented.**

Typical work products include:

- documented test results

Criteria for "Yes" Response:

- ***Each service continuity plan** that supports the critical service is **tested**.*

Criteria for "Incomplete" Response:

- ***Some** service continuity plans are tested.*

4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]

Question Intent: To determine if **backup and storage procedures** for high-value information assets **are tested**.

- Backup and storage of information assets should **meet the requirements** of the service.
- **Testing** of backup and storage procedures is done to **ensure those requirements are being met.**
- Periodic testing of the organization's backup and storage procedures **ensures continued validity as operational conditions change.**

Information asset backup and storage procedures typically include:

- frequency standards
- retention periods
- authorized storage locations and methods
- encryption and protection requirements
- testing standards
- periodic review and revision of backup and storage procedures

Criteria for "Yes" Response:

- *Backup and storage procedures are **tested for all high-value information assets** that support the critical service.*

Criteria for "Incomplete" Response:

- *Backup and storage procedures are tested for **some** high-value information assets.*

5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]

Question Intent: To determine if **test results are compared to test objectives to identify improvements** to service continuity plans.

- The objective of service continuity plan testing is to **ensure that plans work as intended.**
- **Testing identifies required improvements** to the service continuity plans as well as the associated test plans.
- The evaluation of test results involves comparing the documented test results against the established test objectives.
  - Areas where objectives could not be met are recorded, and strategies are developed to review and revise the plans.
  - **Improvements to the testing process** and plans should also be identified, documented, and incorporated into future tests.

Improvement areas may include:

- lack of sufficient resources
- lack of appropriate resources
- training gaps for plan staff and stakeholders
- plan conflicts (if multiple plans are tested simultaneously)
- required changes to infrastructure

Typical work products include:

- documented test results
- list of improvements to service continuity plans
- list of improvements to service continuity test plans

Criteria for "Yes" Response:

- ***Test results for each** service continuity plan required for the delivery of the critical service **are compared with test objectives** to identify needed improvements.*

Criteria for "Incomplete" Response:

- *Test results for **some** service continuity plans are compared with test objectives to identify needed improvements.*

Goal 4 – Service continuity plans are executed and reviewed.

1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]

Question Intent: To determine if **conditions have been identified that trigger the execution** of the service continuity plan.

- The organization must be able to **determine when the plan must be executed** and who is responsible for initiating action.
- The organization should ensure that **owners** of service continuity plans **understand the conditions for execution.**
- Plans may be executed for a variety of reasons, including:
  - in response to a perceived or known threat
  - as a result of an incident
  - in response to a crisis
  - cut-over from one application system to another
  - moving office locations
  - moving data centers

Typical work products include:

- organizational conditions for executing service continuity plans

Criteria for "Yes" Response:

- ***Conditions that trigger the execution*** *of* ***each*** *service continuity plan that supports the critical service have been* ***identified and documented****.*

Criteria for "Incomplete" Response:

- *Conditions that trigger the execution of* ***some*** *service continuity plans have been identified and documented.*

2. Is execution of service continuity plans reviewed? [SC:SG6.SP2]

Question Intent: To determine if the **execution of service continuity plans is reviewed**.

- The **review** of executed service continuity plans **identifies plan shortcomings and needed improvements.**
- **Unforeseen circumstances** that arise during the execution are documented and addressed.

Criteria for "Yes" Response:

- ***The execution of each service continuity plan*** *that supports the critical service* ***is reviewed****.*
- *Or;* ***if service continuity plans have not been executed****, reviews of executed plans are required as part of a standard process.*

Criteria for "Incomplete" Response:

- *The execution of* ***some*** *service continuity plans is reviewed.*

3. Are improvements identified as a result of executing service continuity plans? [SC:SG7.SP2]

Question Intent: To determine if **improvements are identified as a result of executing service continuity plans**.

- **As a result of the review** of executed service continuity plans (SCM:G4.Q2), **improvements are identified and documented.**

Typical work products include:

- list of improvements to service continuity plans
- list of improvements to service continuity test plans

Criteria for "Yes" Response:

- ***Improvements to each executed service continuity plan*** *that supports the critical service* ***are identified and documented****.*
- *Or;* ***if service continuity plans have not been executed****, the identification of improvements to executed plans is required as part of a standard process.*

Criteria for "Incomplete" Response:

- *Improvements to* ***some*** *executed service continuity plans are identified and documented.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing service continuity activities? [SC:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** service continuity management activities **exists**.

- The plan defines service continuity management within the organization and **prescribes how service continuity management activities will be performed.**

- The plan may be a stand-alone document or may be comprised of multiple documents.
- The plan for the service continuity process **details how the organization will perform** service continuity planning, including the development of service continuity plans.
  - The plan for the service continuity process should not be confused with a specific service continuity plan.
  - Service continuity plans are service-specific plans for sustaining services and associated assets.

The plan typically includes:

- service continuity management activities (testing, executing, reviewing both tested and executed plans, identifying improvements, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing service continuity management activities.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for service continuity? [SC:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** service continuity management activities **exists**.

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the service continuity management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform service continuity management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing the service continuity management activities
- communication of plans to stakeholders
- responsibility for testing plans on a regular basis
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations
- post-plan review and revision

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing service continuity management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for service continuity activities been identified and made aware of their roles? [SC:GG2.GP7]

Question Intent: To determine if **stakeholders** for service continuity activities have been **identified** and **made aware of their roles.**

CYBER RESILIENCE **ANALYSIS**

Stakeholders of the service continuity management process have the following **responsibilities**:

- overseeing the service continuity management process
- developing service continuity plans
- coordinating service continuity activities
- participating in the test and execution of service continuity plans
- resolving issues with the service continuity management process
- ensuring that service continuity plans reflect all external dependencies
- reviewing and appraising the effectiveness of service continuity activities

Examples of stakeholders include:

- critical service owners
- management
- owners and custodians of assets that underpin the service
- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- regulatory and legal entities to which the organization is required to submit service continuity plans
- internal and external auditors
- service continuity staff

Criteria for "Yes" Response:

- ***All*** *stakeholders for the service continuity management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the service continuity management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but have* ***not been made aware*** *of their roles.*

4. Have service continuity standards and guidelines been identified and implemented? [SC:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing service continuity management activities **have been implemented**.

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **service continuity management activities meets standards** and is **predictable, measurable**, and **repeatable.**

Standards and guidelines typically address:

- plan ownership
- plan documentation
- plan content
- testing plans, including test objectives, reporting, and frequency
- involvement of stakeholders, including from external dependencies
- plan versioning, storage, archiving, and security
- plan training
- external entities
- issue escalation and resolution procedures

Criteria for "Yes" Response:

- *The organization has **implemented documented standards and guidelines** for performing service continuity management activities.*

Criteria for "Incomplete" Response:

- ***Some** standards and guidelines have been **implemented**.*

MIL3-Managed

1. Is there management oversight of the performance of the service continuity activities? [SC:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists**. The intent of **oversight** is to ensure the **direct, day-to-day monitoring** of the service continuity management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the service continuity management activities.
- **Oversight** provides **visibility** into the service continuity management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the service continuity management activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day service continuity management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day service continuity management activities.*

2. Have qualified staff been assigned to perform service continuity activities as planned? [SC:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff have been assigned**. The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan**.

- Qualified means that **staff are appropriately skilled** to perform service continuity management activities.

Examples of staff include personnel responsible for:

- developing process standards and guidelines
- developing service continuity plans
- developing and conducting service continuity training
- service continuity plan testing and validation
- identifying internal and external dependencies

Examples of skills needed include:

- knowledge necessary to elicit resilience requirements to be reflected in service continuity plans
- knowledge unique to each service that is required to develop service-specific continuity plans
- knowledge necessary to plan and conduct service continuity testing
- knowledge of service continuity tools, techniques, and methods

Criteria for "Yes" Response:

- ***All staff*** *assigned to perform the planned service continuity management activities are* ***appropriately skilled****.*

Criteria for "Incomplete" Response:

- ***Some staff*** *assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform service continuity activities as planned? [SC:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided**. The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of service continuity management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned service continuity management activities include:

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned service continuity management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled? [SC:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the service continuity management activities.

- The intent is to **determine risks that prevent the organization from performing service continuity management activities** (service continuity management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the service continuity management process include:

- poorly defined service continuity management processes
- inadequate staffing
- inadequate funding
- unqualified staff

- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of **all** planned service continuity management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of **some** of the planned service continuity management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned service continuity management activities are **identified but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. **Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results? [SC:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **service continuity management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement**.

Periodic (as defined by the organization) reviews of the service continuity management process are needed to ensure that:

- service continuity performance issues are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to service continuity performance are identified and addressed
- actions requiring management involvement are elevated in a timely manner
- test plans are tested as required
- test results meet objectives
- access to service continuity plans is limited to authorized staff
- changes to service continuity plans are controlled
- the effectiveness of service continuity plans is measured

Example metrics of the service continuity management process may include:

- percentage of service continuity plans completed, tested, executed, and yet to be developed
- percentage of plans that meet objectives (e.g., RTOs and RPOs)
- percentage of plans that require changes to meet objectives
- percentage of plans that have not been reviewed post-test or post-execution
- percentage of staff who have not been trained

Criteria for "Yes" Response:

- ***All** service continuity management activities are **periodically** (as defined by the organization) **reviewed** and **measured** and the **results evaluated**.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review of the service continuity management activities.*

- *Or; review and measurement address **some** of the service continuity management activities.*
- *Or; service continuity management activities are **reviewed but not measured**.*

2. Are service continuity activities periodically reviewed to ensure they are adhering to the plan? [SC:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To **periodically** determine if service continuity management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the service continuity management plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing service continuity management activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- ***All** service continuity management activities are **periodically (as defined by the organization) reviewed** to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review.*
- *Or; **some** service continuity management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of service continuity? [SC:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of service continuity management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the service continuity management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes:

- reviews of **status** of service continuity management activities
- **issues** identified in process and plan reviews
- **risks** associated with service continuity management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is **made aware of issues** related to the performance of service continuity management through **scheduled** communication.*

Criteria for "Incomplete" Response:

- *The organization has **not established a frequency** for communication to higher-level management.*
- *Or; communications address **some** issues.*

CYBER RESILIENCE ANALYSIS

MIL5-Defined

1. **Has the organization adopted a standard definition of service continuity activities from which operating units can derive practices that fit their unique operating circumstances? [SC:GG3.GP1],[GG3.GP1]**

Question Intent: To determine if the organization has a **standard process** that defines service continuity management.

- **A standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in service continuity management activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed
- process flow, including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of service continuity management.*

Criteria for "Incomplete" Response:

- *A standard definition of service continuity management is **in development and partially documented**.*

2. **Are improvements to service continuity documented and shared across the organization? [SC:GG3.GP2],[GG3.GP2]**

Question Intent: To ensure that **improvements** to the service continuity management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the service continuity management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include:

- process metrics and measurements
- lessons learned from testing and executing service continuity plans
- improvements based on risk identification and mitigation
- lessons learned from conflicts arising from resource contention between service continuity plans

Criteria for "Yes" Response:

- ***Improvements** to service continuity management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to service continuity management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

CYBER RESILIENCE
ANALYSIS

7 Risk Management

The purpose of Risk Management is to identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.

Goals and Practices

Goal 1 – A strategy for identifying, analyzing, and mitigating risks is developed.

1. Have sources of risk that can affect operations been identified? [RISK: SG1.SP1]

Question Intent: To determine if **sources of risk that can affect operations have been identified**.

- **Operational risk** is defined as the **potential impact** on assets and the related services—the risk that results from operating services and assets on a day-to-day basis.
- **Operational risk sources** are the fundamental areas of risk that can affect the critical service and associated assets.
- **Identifying risk sources or areas of risk** helps the organization determine and categorize the types of operational risk that are most likely to affect day-to-day operations.

Risk sources typically include:

- poorly designed and executed business processes and services
- inadvertent actions of people, such as accidental disclosures or modifications of information
- intentional actions of people, such as insider threat and fraud
- failure of systems to perform as intended
- failures of technology, such as the unanticipated results of the execution of software
- external events and forces, such as natural disasters, failures of public infrastructure, and failures in the organization's supply chain

Criteria for "Yes" Response:

- ***Sources of risk*** *that can affect operation of the critical service* ***have been identified and documented****.*

Criteria for "Incomplete" Response:

- *Sources of risk that can affect operation of the critical service are* ***being identified and are partially documented****.*

2. Have categories been established for risks? [RISK: SG1.SP1]

Question Intent: To determine if **categories have been established for risks**.

- **Risk categories** provide a means for collecting and organizing risk for ease of analysis and mitigation.
- Operational risk categories **typically align with the sources of operational risk.**
- Risk categories **can be as granular as necessary** for the organization to effectively manage risk.

Examples of operational risk categories:

- failed processes
  - employee screening
  - vendor management

- actions of people
  - malicious attack
  - inadvertent disclosure
- systems and technology
  - unsupported software
  - hardware failure
- external events
  - natural disaster
  - supply chain interruption

Criteria for "Yes" Response:

- ***Categories of risk*** *that can affect the critical service* ***have been established and documented****.*

Criteria for "Incomplete" Response:

- *Categories of risk that can affect the critical service* ***are being established and are partially documented****.*

3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]

Question Intent: To determine if a **plan for managing operational risk has been established**.

- **The plan provides a common foundation** for the performance of operational risk management activities.
- The operational risk management plan should be developed to **facilitate the accumulation of operational risks as input** to the organization's enterprise risk management program.

Typical items addressed in an operational risk management plan include:

- the scope of operational risk management activities
- the methods to be used for operational risk identification, analysis, mitigation, monitoring, etc.
- identification of sources of operational risk
- risk mitigation techniques to be used
- identification and definition of risk metrics
- frequency of risk monitoring and reassessment

Criteria for "Yes" Response:

- *There is a* ***documented plan for managing operational risk****.*

Criteria for "Incomplete" Response:

- *A plan is* ***in development and partially documented****.*

4. Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]

Question Intent: To determine if the **plan for managing operational risk is communicated to stakeholders.**

- Relevant stakeholders can be internal or external to the organization and are responsible for operational risk management activities.

Criteria for "Yes" Response:

- ***The plan*** *for managing operational risk is* ***communicated to all stakeholders*** *that support the critical service.*

Criteria for "Incomplete" Response:

- *The plan for managing operational risk is communicated to* ***some*** *stakeholders.*

CYBER RESILIENCE **ANALYSIS**

Goal 2 – Risk tolerances are identified, and the focus of risk management activities is established.

1. Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]

Question Intent: To determine if **impact areas have been identified**, such as reputation, financial health, and regulatory compliance.

- **Organizational impact areas** identify the categories where realized risk may have meaningful and disruptive consequences.
- **Impact areas reflect what is important to the organization** and to the accomplishment of its mission.
- Organizational impact areas **help identify how realized risk may affect the organization.**

Examples of organizational impact areas:

- reputation and customer confidence
- revenue
- staff productivity
- safety and health of staff and customers
- fines and legal penalties
- compliance with regulations

Criteria for "Yes" Response:

- *Impact areas have been **identified and documented** for the critical service.*

Criteria for "Incomplete" Response:

- *Impact areas are **being identified and are partially documented**.*

2. Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]

Question Intent: To determine if **impact areas have been prioritized to determine their relative importance**.

- Prioritization allows the organization to determine the **relative importance of impact areas for risk prioritization and mitigation.**

Criteria for "Yes" Response:

- *The organization has **prioritized all impact areas** (documented in G2.Q1) that affect the critical service.*

Criteria for "Incomplete" Response:

- *The organization has prioritized **some** impact areas that affect the critical service.*

3. Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]

Question Intent: To determine if **risk tolerance parameters have been established for each impact area**.

- Risk parameters **may differ for each impact area.**
- Risk parameters **provide the organization a means for consistent measurement** of risk across the organization.
- **Risk tolerance parameters describe the risk measurement criteria** for each impact area.
- **Risk measurement criteria include** how impact is measured, how frequently it is measured, and what is to be measured.
- Risk tolerance parameters can be **qualitative** (high, medium, low) or **quantitative** (based on levels of loss, fines, number of customers lost, etc.).

Criteria for "Yes" Response:

- *The organization has **established risk tolerance parameters for each impact area** defined for the critical service.*

Criteria for "Incomplete" Response:

- *The organization has established risk tolerance parameters for **some** impact areas.*

4. Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]

Question Intent: To determine if **risk tolerance thresholds, which trigger action, are defined for each category of risk**.

- Risk tolerance parameters describe the risk measurement criteria for each impact area.
- **Risk tolerance thresholds** are used by management to determine when a risk is in control or when it has exceeded acceptable limits.
- Risk tolerance thresholds **should be set for each category of risk** that the organization establishes as a means for measuring and managing risk. For example:
  - A risk tolerance threshold for a category of risk may be whenever more than 200 users are impacted.
  - The risk tolerance threshold indicates when action needs to be taken to prevent operational disruption.

Criteria for "Yes" Response:

- *The organization has **established a risk tolerance threshold for each category of risk** defined for the critical service.*

Criteria for "Incomplete" Response:

- *The organization has established a risk tolerance threshold for **some** categories of risk defined for the critical service.*

Goal 3 – Risks are identified.

1. Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]

Question Intent: To determine if **operational risks that could affect delivery of the critical service are identified**.

- From the sources and categories of risk established in G1.Q1 and G1.Q2, **specific risks that affect the delivery of the critical service should be identified.**
- The organization should determine the effect on the service that could result from the realization of risk at the asset level.

Typical Work Products:

- List of operational risks by service

Criteria for "Yes" Response:

- ***Operational risks** that could affect delivery of the critical service are **identified and documented**.*

Criteria for "Incomplete" Response:

- *Operational risks that could affect delivery of the critical service are being **identified and are partially documented**.*

Goal 4 – Risks are analyzed and assigned a disposition.

1. Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if **risks are analyzed to determine the potential impact to the critical service**.

- Each **risk (identified in RM:G3.Q1) should be evaluated** and assigned values in accordance with the defined risk parameters to determine impact to the critical service.
- The organization should **determine if the impact of the risk would exceed the risk tolerance thresholds.**

Typical Work Products:

- Business Impact Analysis
- Updated operational risk statements to include the impact valuation. Risk statements may include:
  - asset affected
  - weakness or vulnerability
  - means of exploitation
  - likelihood (if known)
  - undesired outcomes or impacts
  - consequence to the organization

Criteria for "Yes" Response:

- ***All identified risks to the critical service are analyzed*** *to determine the potential impact.*

Criteria for "Incomplete" Response:

- ***Some*** *identified risks to the critical service are analyzed to determine the potential impact.*

2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]

Question Intent: To determine if a **disposition is assigned to identified risks.**

- A disposition is a **statement of how the organization intends to address the risk.**
- A risk disposition should be **assigned to each operational risk.**

Risk dispositions typically include:

- **Avoid** – altering operations to avoid the risk while still providing the service
- **Accept** – acknowledging the risk without taking action
- **Monitor** – deferring action until there is a need to address the risk
- **Transfer** – assigning the risk to a willing and able entity
- **Mitigate or control** – taking active steps to minimize the risk

Criteria for "Yes" Response:

- *A* ***disposition is assigned to all identified risks*** *that affect the critical service.*

Criteria for "Incomplete" Response:

- *A disposition is assigned to* ***some*** *identified risks that affect the critical service.*

Goal 5 – Risks to assets and services are mitigated and controlled.

1. Are plans developed for risks that the organization decides to mitigate? [RISK: SG5.SP1]

Question Intent: To determine if **plans are developed for risks that the organization decides to mitigate**.

- **Risk mitigation plans should be developed** when operational risk exceeds the organization's risk threshold and are determined to be unacceptable.

Risk mitigation plans may include actions to:

- **reduce the likelihood** (probability) of the vulnerability or threat and resulting risk
- **minimize exposure** to the vulnerability or threat from which the risk arises
- **develop service continuity plans** that would keep an asset or service in production if affected by realized risk
- **develop recovery and restoration plans** to address the consequences of realized risk

Criteria for "Yes" Response:

- ***Risk mitigation plans are developed and documented*** *for* ***all risks*** *that the organization decides to mitigate.*

Criteria for "Incomplete" Response:

- *Risk mitigation plans are* ***in development and partially documented****.*

2. Are identified risks tracked to closure? [RISK: SG5.SP2]

Question Intent: To determine if **identified risks are tracked to closure.**

- **The disposition of risks must be tracked, periodically assessed, and revised as necessary.**
- **The organization should provide a method for tracking open risks to closure.**

Criteria for "Yes" Response:

- ***All*** *identified risks are tracked to closure.*

Criteria for "Incomplete" Response:

- ***Some*** *identified risks are tracked to closure.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing risk management activities? [RISK:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** risk management **exists.**

- The plan defines risk management within the organization and **prescribes how risk management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- risk management activities (risk identification, risk analysis, and risk mitigation)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a* ***documented plan*** *for performing risk management.*

Criteria for "Incomplete" Response:

- *A plan is* ***in development and partially documented****.*

2. Is there a documented policy for risk management? [RISK:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** risk management activities **exists.**

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the risk management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform risk management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing the risk environment
- measuring adherence to policy, when exceptions are granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing risk management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for risk management activities have identified and made aware of their roles? [RISK:GG2:GP7]

Question Intent: To determine if **stakeholders** for risk management activities have been **identified** and **made aware of their roles.**

Stakeholders of the risk management process have the following **responsibilities**:

- identifying risk
- analyzing risk
- developing and implementing risk mitigation plans
- reviewing the effectiveness of the risk management process
- managing the risk resulting from unresolved problems (gaps in processes, insufficient staffing or funding, etc.)

Examples of stakeholders include**:**

- critical service owners
- management
- owners and custodians of assets that underpin the service
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors

Criteria for "Yes" Response:

- ***All** stakeholders for the risk management activities have been **identified** and **made aware** of their roles.*

Criteria for "Incomplete" Response:

- ***Some** stakeholders for the risk management activities have been **identified** and **made aware** of their roles.*
- *Or; stakeholders are identified but have **not been made aware** of their roles.*

4. Have risk management activities standards and guidelines been identified and implemented? [RISK:GG2.GP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if **standards and guidelines** for performing risk management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **risk management activities meets standards** and is **predictable, measurable**, and **repeatable.**

Standards and guidelines typically address:

- identifying risk sources and categories of risk
- defining risk parameters (such as risk tolerance thresholds) and risk measurement criteria
- assigning risk priorities based on risk analysis
- assigning risk dispositions
- developing risk mitigation plans

Criteria for "Yes" Response:

- *The organization has **implemented documented standards and guidelines** for performing risk management activities.*

Criteria for "Incomplete" Response:

- ***Some** standards and guidelines have been **implemented**.*

MIL3-Managed

1. Is there management oversight of the performance of the risk management activities? [RISK:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of risk management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of risk management activities.
- **Oversight** provides **visibility** into risk management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of Corrective Actions:

- taking actions to repair defective work products (risk statements, risk disposition, risk mitigation plans, documentation)
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in risk management activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day risk management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day risk management activities.*

2. Have qualified staff been assigned to perform risk management activities as planned? [RISK:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan.**

- "Qualified" means that **staff are appropriately skilled** to perform risk management activities.

Examples of staff include personnel responsible for:

- identifying operational risk sources and categories
- assessing operational risks
- business impact analysis
- developing risk mitigation plans
- monitoring and tracking risk to closure

Examples of skills needed include:

- proficiency with tools, techniques, and methods used to identify, analyze, mitigate, and monitor operational risk
- knowledge necessary to develop, implement, and monitor risk mitigation plans
- strong communication skills for conveying the operational risk and mitigation plans to higher level managers

Criteria for "Yes" Response:

- ***All staff*** *assigned to perform the planned risk management activities are* ***appropriately skilled****.*

Criteria for "Incomplete" Response:

- ***Some staff*** *assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform risk management activities as planned? [RISK:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided.** The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of risk management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned risk management activities include**:**

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities, including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned risk management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled? [RISK:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of risk management activities**.**

- The intent is to **determine risks that prevent the organization from performing risk management activities** (risk management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the risk management process include:

- poorly defined risk management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of **all** planned risk management activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of **some** of the planned risk management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or risks to the performance of planned risk management activities are **identified, but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results? [RISK:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To ensure the **risk management activities (process) remain effective** and **produce the intended results** by **conducting periodic reviews** and **measurement activities.**

Periodic (as defined by the organization) reviews of the risk management process are needed to ensure that**:**

- the performance of risk management process activities is being monitored and regularly reported
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- actions requiring management involvement are elevated in a timely manner

Example metrics of the risk management process may include:

- percentage of identified assets and services for which some form of risk assessment has been performed and documented
- percentage of identified assets and services for which the impact or cost of compromise has been quantified
- percentage of identified risks that have not been tracked to closure
- percentage of identified risks that do not have a defined risk disposition

Criteria for "Yes" Response:

- ***All** risk management activities are **periodically** (as defined by the organization) **reviewed** and **measured** and the **results are evaluated**.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review of risk management activities.*
- *Or; review and measurement addresses **some** of the risk management activities.*
- *Or; risk management activities are **reviewed but not measured**.*

2. Are risk management activities periodically reviewed to ensure they are adhering to the plan? [RISK:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To **periodically** determine if risk management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the risk management plan are needed to **ensure that:**

- activities are **performed as planned and adhere to process descriptions, standards, and procedures**
- deviations from the plan are identified and evaluated
- problems in the plan for performing risk management activities are identified
- non-compliance is addressed
- needed process changes are identified when expected results or outputs are not met

Criteria for "Yes" Response:

- ***All** risk management activities are **periodically (as defined by the organization) reviewed** to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review.*
- *Or; **some** risk management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of risk management? [RISK:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of risk management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the risk management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher level managers typically includes**:**

- **status reviews** of risk management activities
- **issues** identified in process and plan reviews
- **risks** associated with risk management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is **made aware of issues** related to the performance of risk management through **scheduled** communication.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for communication to higher-level management.*
- *Or; communications address **some** issues.*

CYBER RESILIENCE ANALYSIS

MIL5-Defined

1. **Has the organization adopted a standard definition of risk management activities from which operating units can derive practices that fit their unique operating circumstances? [RISK:GG3.GP1],[GG3.GP1]**

Question Intent: To determine if the organization has a **standard process** that defines risk management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in risk management activities across the organization.

A **standard definition** may include**:**

- process description
- process activities and practices to be performed
- process flow, including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of risk management.*

Criteria for "Incomplete" Response:

- *A standard definition of risk management is **in development and partially documented**.*

2. **Are improvements to risk management documented and shared across the organization? [RISK:GG3.GP2],[GG3.GP2]**

Question Intent: To ensure that **improvements** to the risk management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the risk management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include**:**

- process metrics and measurements
- lessons learned from both successfully and unsuccessfully mitigating identified risks
- issues with the risk identification, analysis, prioritization, assessment, mitigation, and monitoring processes

Criteria for "Yes" Response:

- ***Improvements** to risk management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to risk management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*

CYBER RESILIENCE
ANALYSIS

8 External Dependencies Management

The purpose of External Dependencies Management is 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.

Goals and Practices

Goal 1 – External dependencies are identified and prioritized to ensure sustained operation of high-value services.

1. Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1]

Question Intent: To determine if **external dependencies** that are critical to the service are **identified**.

- **An external dependency exists when** an external entity (contractor, customer, service provider, etc.)
  - has access to
  - control of
  - ownership in
  - possession of
  - responsibility for
  - or other defined obligations related to the critical service or its associated assets

Examples of services provided to an organization from external entities can include:

- outsourced activities that support operation or maintenance of the critical service
- security operations, IT service delivery and operations management, or services that directly affect resilience processes
- backup and recovery of data, provision of backup facilities for operations and processing, and provision of support technology, or similar resilience-specific services
- infrastructure providers such as power and dark fiber
- telecommunications (telephony and data)
- public services such as fire and police support, emergency medical services, and emergency management services
- technology and information assets, such as application software and databases

Typical work products include:

- list of external dependencies and entities

Criteria for "Yes" Response:

- *The organization has **documented all** external dependencies that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **documented some** of the external dependencies.*

2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]

Question Intent: To determine if a **process for creating and maintaining** the **list of external dependencies exists**.

- The organization's external dependencies will **change over time as a result of changes to relationships** with suppliers and customers, changes in services, the lifecycle of assets, etc.
- Once the list of external dependencies is established, it is **important that it be maintained.**
- A process for **updating the list on a regular basis** should be established.

Typical work products include:

- documented process for creating and maintaining the list of external dependencies

Criteria for "Yes" Response:

- *The organization has **established a process** for creating and maintaining the list of external dependencies that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has a **process in development and partially documented**.*

3. Are external dependencies prioritized? [EXD:SG1.SP2]

Question Intent: To determine if **external dependencies are prioritized.** The intent of **prioritization** is to ensure that the organization **properly directs** its **resources** to the external dependencies that **most directly impact the critical service**.

Prioritization criteria may include dependencies that:

- directly affect the operation and delivery of the critical service
- support, maintain, or have custodial care of critical service assets
- support the continuity of operations of the critical service
- have access to highly sensitive or classified information
- support more than one critical service
- supply assets that support the operation of a critical service
- impact the recovery time objective of the critical service

Typical work products include:

- criteria for prioritizing external dependencies
- prioritized list of external dependencies

Criteria for "Yes" Response:

- *The organization has a **prioritized list** of **all** external dependencies that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **prioritized some** external dependencies.*

Goal 2 – Risks due to external dependencies are identified and managed.

1. Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]

Question Intent: To determine if **risks** due to external dependencies are **identified and managed**. The intent of managing risk is to ensure the continuous operation of the critical service.

- The identification of risks due to external dependencies forms a baseline from which a continuous risk management process can be established and managed.

Examples of risk include:

- financial conditions
- availability of external staff
- reliance on subcontractors
- risks to assets owned or operated by external entities
- scalability of the external entity to meet capacity requirements
- ability to support the continuity of operations of the critical service

Typical work products include:

- external dependency risk statements, with impact valuation
- list of external dependency risks, with categorization and prioritization
- vendor management process to identify and evaluate risk

Criteria for "Yes" Response:

- *The organization has **identified risks** associated with **all** external dependencies that support the critical service.*
- *And; **risks are managed** (impacts identified, analyzed, and the disposition of risk has been assigned).*

Criteria for "Incomplete" Response:

- *The organization has **identified and managed risks associated with some** of the external dependencies.*

Goal 3 – Relationships with external entities are formally established and maintained.

1. Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]

Question Intent: To determine if **resilience requirements** for **each** external dependency have been **established**.

- For each external dependency, the organization should **establish** a detailed set of **resilience (protection and sustainment) requirements** that the external entity must meet to support the critical service.

When developing protection and sustainment requirements for external dependencies, the organization should:

- consider the external entity's impact on the operation of the critical service
- consider the external entity's impact on the sustainability and recovery of the critical service
- consider regulatory obligations
- consult internal and external stakeholders responsible for the associated assets and services
- consider other critical services that rely upon the same external dependency
- include enterprise-level requirements

Typical work products include:

- documented resilience requirements of the critical service:
  - Availability
  - Security
  - Integrity
  - RPO/RTO
  - Backup Requirements

Criteria for "Yes" Response:

- *The organization has established resilience requirements that **apply to each** external entity that supports the critical service.*

Criteria for "Incomplete" Response:

- *The organization has established resilience requirements that **apply to some** of the external entities.*

2. Are these requirements reviewed and updated? [EXD:SG3.SP2]

Question Intent: To determine if the organization**, reviews and updates** resilience requirements.

- Typically this would be done periodically (as defined by the organization).
- This can also be done as conditions warrant. Example conditions:
  - Change in external entity relationship
  - Change in the critical service operating environment that may affect the resilience requirements.

Criteria for "Yes" Response:

- *The organization **reviews and updates** the resilience requirements for **all** external entities that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization **reviews and updates** the resilience requirements for **some** external entities.*

3. Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]

Question Intent: To determine if the **ability of an external entity to meet resilience requirements** is considered in the selection process.

- The selection process and criteria should be designed to **ensure** that the selected entity can **fully meet** the organization's established **requirements.**

Typical work products include:

- requests for proposals or other types of solicitation documents that include resilience requirements
- external entity selection criteria
- evaluation of each external entity proposal against the selection criteria

Criteria for "Yes" Response:

- *The ability to meet resilience requirements **is considered** when selecting **all** external entities that will support the critical service.*

Criteria for "Incomplete" Response:

- *The ability to meet resilience requirements **is considered** when selecting **some** external entities.*

4. Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]

Question Intent: To determine if **resilience requirements** are **reflected in agreements** with external entities.

- Protection and sustainment **requirements** included in agreements will form the **basis for monitoring the performance** of the external entity.

Types of agreements may include:

- contracts
- service level agreements
- memoranda of agreement
- purchase orders
- licensing agreements

The agreement should:

- be enforceable by the organization
- include detailed and complete requirements that must be met by the external entity
- include required performance standards and/or work products
- be updated to reflect changes in requirements over the life of the relationship

Example resilience requirements can include:

- performance standards
- security, confidentiality, and privacy requirements
- disclosure obligations for security breaches
- business resumption and contingency plans
- staff performance or prescreening
- controls
- regulatory, legal, and compliance obligations

Typical work products include:

- agreements with external entities
- service level agreements
- requirements traceability matrix
- resilience requirements specification

Criteria for "Yes" Response:

- *The organization **includes** resilience requirements in agreements with **all** external entities that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization **includes** resilience requirements in agreements with **some** external entities.*

Goal 4 – Performance of external entities is managed.

1. Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]

Question Intent: To determine if the **performance** of external entities is **monitored** against the requirements of the critical service.

- Typically performance would be reviewed periodically (as defined by the organization).
- Performance reviews can also be done as conditions warrant. Example conditions:
  - Sudden change in external entity performance
  - Change in the expected quality of work products.
- Protection and sustainment **requirements** included in agreements should be **used as the basis for monitoring the performance** of the external entity.
- This **includes all services provided in support of the critical service** for which the external entity is responsible.

- Any **deviations** from established agreements must be **analyzed** to understand the potential impact on the organization.

Criteria for "Yes" Response:

- *The organization **monitors** the **performance** of **all** external entities that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization **monitors** the performance of **some** external entities.*

2. Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]

Question Intent: To determine if **responsibility** for monitoring external entities is **assigned.**

- **Assigning responsibility** ensures that monitoring is performed on a timely and consistent basis.
- The organization should **assign responsibility** for monitoring each **entity.**
- Responsibility is typically **assigned** to the **owner of the relationship.**
- The responsible staff should **establish procedures** that determine the **frequency, protocol, and responsibility for monitoring** a particular external entity.
- These procedures should be **consistent with the terms of the agreement** with the external entity.

Criteria for "Yes" Response:

- *The **responsibility for monitoring** the performance of **each** external entity that supports the critical service has been **assigned.***

Criteria for "Incomplete" Response:

- *The **responsibility for monitoring** the performance of **some** external entities has been **assigned**.*

3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]

Question Intent: To determine if **corrective actions are taken** to address issues with the performance of external entities (as related to resilience requirements). The intent of any corrective action is to minimize disruption to the critical service.

- The **range of corrective actions** should be **established** in the agreement with the external entity.

Typical work products include:

- corrective action reports or documentation
- correspondence with an external entity documenting corrective actions

Criteria for "Yes" Response:

- *The organization has **taken corrective actions** to address **performance issues** for **all** external entities that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **taken corrective actions** to address **performance issues** for **some** external entities.*

4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]

Question Intent: To **evaluate if the issues** with external entity performance have been **remedied** by the corrective actions.

Criteria for "Yes" Response:

- *The organization has **evaluated corrective actions** that address performance issues for **all** external entities supporting the critical service.*

Criteria for "Incomplete" Response:

- *The organization has **evaluated corrective actions** that address performance issues for **some** external entities.*

Goal 5 – Dependencies on public services and infrastructure service providers are identified.

1. Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]

Question Intent: To determine if **public services** that the **critical service depends** on are **identified.**

- **Public services may be vital** to a facility's continued operation during a disruption.
- Thorough consideration of these services must be given for **service continuity planning.**
- Public services generally include services that are **specific to the geographical region** of the facility.

Public services include:

- fire response and rescue services
- local and federal law enforcement (police, National Guard, FBI, etc.)
- emergency management services, including paramedics and first responders
- other services, such as hazardous material control

Typical work products include:

- results of business impact analysis (documenting public service dependencies for facilities)
- list of public service providers on which facilities are dependent
- key contact list
- updated service continuity plans

Criteria for "Yes" Response:

- *The organization has **identified and documented all** public services on which the critical service depends.*

Criteria for "Incomplete" Response:

- ***Some** public services are identified.*

2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]

Question Intent: To determine if **infrastructure providers** that the **critical service depends** on are **identified.**

- **Critical services may be dependent on infrastructure providers** to remain viable.
- The organization must be prepared to **address the loss of these providers**, which can affect the resilience of the critical service.
- The organization may need to **consider the resilience of the providers when developing service continuity plans.**

These infrastructure services include:

- telecommunications and telephone services
- data and network service providers
- electricity, natural gas, and other energy sources
- water and sewer services
- fuel providers for emergency power

Typical work products include:

- results of business impact analysis (documenting infrastructure dependencies for the critical service)
- list of infrastructure providers on which the critical service depends
- key contact list
- updated service continuity plans

Criteria for "Yes" Response:

- *The organization has **identified and documented all** infrastructure providers on which the critical service depends.*

Criteria for "Incomplete" Response:

- ***Some** infrastructure providers are identified.*

Maturity Indicator Levels

MIL2-Planned

1. **Is there a documented plan for performing external dependency management activities? [EXD:GG2.GP2],[GG2.GP2]**

Question Intent: To determine if a **plan for performing** external dependency management activities **exists.**

- The plan defines external dependency management within the organization and **prescribes how external dependency management activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.
- A vendor management or contract management program and plan may suffice if it encompasses planning elements similar to those listed below.

The plan typically includes:

- external dependency management activities (external dependency identification, prioritization, performance management, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders
- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing external dependency management.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. **Is there a documented policy for external dependency management? [EXD:GG2:GP1.SP2],[GG2:GP1]**

CYBER RESILIENCE **ANALYSIS**

Question Intent: To determine if a **policy for performing** external dependency management activities **exists.**

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the external dependency management process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform external dependency management activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing the external dependency management activities
- requesting, approving, providing, and terminating access for external entities
- requesting, approving, providing, and terminating agreements with external entities
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing external dependency management.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for external dependency management activities been identified and made aware of their roles? [EXD:GG2.GP7]

Question Intent: To determine if **stakeholders** for external dependency activities have been **identified** and **made aware of their roles.**

Stakeholders of the external dependency management process have the following **responsibilities**:

- overseeing the external dependency management process
- resolving issues with the external dependency management process
- planning for evaluating, selecting, and managing relationships with external entities
- creating and maintaining a prioritized inventory of all external dependencies
- monitoring the performance of external entities
- ensuring that service continuity plans reflect all external dependencies
- managing the operational risk that arises from external dependencies

Examples of stakeholders include:

- critical service owners
- management
- owners of external entity relationships
- external dependency management program staff
- owners and custodians of assets that underpin the service
- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors
- acquisition and procurement staff
- service continuity staff

Criteria for "Yes" Response:

- ***All*** *stakeholders for the external dependency management activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the external dependency management activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but* ***have not been made aware*** *of their roles.*

4. Have external dependency management activities standards and guidelines been identified and implemented? [EXD:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing external dependency management activities **have been implemented.**

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **external dependency management activities meets standards** and is **predictable, measurable**, and **repeatable.**

Standards and guidelines typically address:

- identifying and prioritizing external dependencies
- associating external dependencies with services and assets
- managing operational risks resulting from external entities
- evaluating and selecting external entities
- standards of performance and service levels
- periodically monitoring the performance of external entities
- establishing service continuity plans and procedures for external entities
- terminating relationships with entities
- issue escalation and dispute resolution procedures

Criteria for "Yes" Response:

- *The organization has* ***implemented documented standards and guidelines*** *for performing external dependency management activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented****.*

MIL3-Managed

1. Is there management oversight of the performance of the external dependency management activities? [EXD:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists.** The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the external dependency management activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the external dependency management activities.

- **Oversight** provides **visibility** into the external dependency management activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products or services
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)
- identifying improvements in the external dependency management activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day external dependency management activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day external dependency management activities.*

2. Have qualified staff been assigned to perform external dependency management activities as planned? [EXD:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff have been assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan.**

- Qualified means that **staff are appropriately skilled** to perform external dependency management activities.

Examples of staff include personnel responsible for:

- preparing request for proposals (RFPs), including applicable service level agreements (SLAs)
- evaluating proposals and selecting external entities
- establishing formal agreements with external entities
- inspecting deliverables
- monitoring the performance of external entities
- service continuity as it involves external dependencies

Examples of skills needed include:

- identifying and prioritizing external dependencies
- elicitation of resilience specifications to be reflected in RFPs and agreements
- evaluating and selecting external entities
- managing relationships with external entities
- negotiating agreements with external entities

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned external dependency management activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff*** *assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform external dependency management activities as planned? [EXD:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided.** The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of external dependency management activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned external dependency management activities include:

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned external dependency management activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned external dependency management activities identified, analyzed, disposed of, monitored, and controlled? [EXD:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the external dependency management activities**.**

- The intent is to **determine risks that prevent the organization from performing external dependency management activities** (external dependency management process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the external dependency management process include:

- poorly defined external dependency management processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned external dependency management activities are identified, analyzed, disposed of, monitored, and controlled.*

CYBER RESILIENCE **ANALYSIS**

Criteria for "Incomplete" Response:

- *Risks to the performance of **some** of the planned external dependency management activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned external dependency management activities are **identified, but are not** analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. **Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results? [EXD:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **external dependency management activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement.**

Periodic (as defined by the organization) reviews of the external dependency management process are needed to ensure that:

- external dependency performance issues are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to external dependency performance are identified and addressed
- actions requiring management involvement are elevated in a timely manner
- new external dependencies are included and prioritized
- agreements with external entities include stated resilience requirements
- the mapping of external dependencies to services and assets is accurate and current

Example metrics of the external dependency management process may include:

- number of performance issues resulting from external entity monitoring
- percentage of external entities whose deliverables do not meet expectations
- number of external dependency risks where corrective action is still pending
- level of adherence to external dependency related policies

Criteria for "Yes" Response:

- ***All** external dependency management activities are **periodically** (as defined by the organization) **reviewed** and **measured** and the **results evaluated**.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for review of the external dependency management activities.*
- *Or; review and measurement address **some** of the external dependency management activities.*
- *Or; external dependency management activities are **reviewed but not measured**.*

2. **Are external dependency management activities periodically reviewed to ensure they are adhering to the plan? [EXD:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

CYBER RESILIENCE **ANALYSIS**

Question Intent: To **periodically** determine if external dependency management activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the external dependency management plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing external dependency management activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- ***All*** *external dependency management activities are* ***periodically (as defined by the organization) reviewed*** *to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review.*
- *Or;* ***some*** *external dependency management activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to external dependency management? [EXD:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of external dependency management is **communicated** to higher-level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher-level managers include those in the organization **above the immediate level of management** responsible for the external dependency management process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher-level managers typically includes:

- **status reviews** of external dependency management activities
- **issues** identified in process and plan reviews
- **risks** associated with external dependency management activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is* ***made aware of issues*** *related to the performance of external dependency management through* ***scheduled*** *communication.*

Criteria for "Incomplete" Response:

- *The organization has* ***not established a frequency*** *for communication to higher-level management.*
- *Or; communications address* ***some*** *issues.*

CYBER RESILIENCE ANALYSIS

MIL5-Defined

1. **Has the organization adopted a standard definition of the external dependency management activities from which operating units can derive practices that fit their unique operating circumstances? [EXD:GG3.GP1],[GG3.GP1]**

Question Intent: To determine if the organization has a **standard process** that defines external dependency management.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in external dependency management activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed
- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of external dependency management.*

Criteria for "Incomplete" Response:

- *A standard definition of external dependency management is **in development and partially documented**.*

2. **Are improvements to external dependency management documented and shared across the organization? [EXD:GG3.GP2],[GG3.GP2]**

Question Intent: To ensure that **improvements** to the external dependency management process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the external dependency management process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include**:**

- process metrics and measurements
- lessons learned in post-event review of external entity incidents and disruptions in continuity
- lessons learned in managing an external entity
- improvements based on risk identification and mitigation
- improvements based on executed or tested service continuity plans that rely on external entities

Criteria for "Yes" Response:

- ***Improvements** to external dependency management processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to external dependency management processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization*

CYBER RESILIENCE
ANALYSIS

9 Training and Awareness

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

Goals and Practices

Goal 1 – Cyber security awareness and training programs are established.

1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]

Question Intent: To determine if **cyber security awareness needs have been identified** for the critical service.

- Awareness differs from skill based training; it **focuses on making staff more cognizant of their cyber security responsibilities.**
- To establish an effective awareness program, an organization **must identify awareness needs** and **establish a plan and capability** to meet those needs.
- **Awareness activities** focus on staff members developing an understanding of issues, concerns, policies, plans, and practices related to the resilience of the critical service.

Awareness sources for the critical service may include:

- resilience requirements (protection and sustainment requirements for assets and services)
- organizational policies
- vulnerabilities being actively managed
- laws and regulations (confidentiality and privacy regulations, other federal, state, and local laws that restrict disclosure of information or modification of information)
- service continuity and communication plans
- event reporting procedures

Criteria for "Yes" Response:

- *The organization has **identified all** of the **cyber security awareness needs** for the critical service.*

Criteria for "Incomplete" Response:

- *The organization has identified **some** of the cyber security awareness needs.*

2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP1]

Question Intent: To determine if the **required skills** necessary to fulfill specific roles that support the critical service **have been identified**.

- In order to determine what skills the organization must possess to meet its cyber security needs, **baseline competencies must be established** for the critical service.
- **Baseline competencies represent the staffing and skill set needs**, not what it currently has in terms of staff and skills.
- By determining the required skills, the appropriate target for a sufficient level of staffing and skills is established.

Sources of baseline competencies may include:

- role (security administrator, network administrator, CIO, etc.)
- position (CIO, senior security analyst, network engineer, etc.)
- organizational processes such as vulnerability management, incident management, service continuity management, etc.
- skills (Java programming, Oracle DBA, etc.)
- certifications (CISSP, MSCE, etc.)
- aptitudes and job requirements (able to work long hours, travel, or be on call)

Criteria for "Yes" Response:

- *The organization has **identified all required skills** for the specific roles needed to support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has identified **some** required skills for the specific roles.*

3. Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]

Question Intent: To determine if **skill gaps** present in personnel responsible for cyber security of the critical service have been **identified**.

- The organization must **determine what skills it currently possesses** in the assigned personnel and **identify skill gaps** that can affect their ability to perform assigned cyber security tasks in support of the critical service.
- The differences, if any, between the skills the organization currently possess and the required skills (established in TA:G1.Q2) represent skill gaps.
- Skill gaps and deficiencies **expose the areas where the organization does not have the expertise or experience** to meet current needs.
- When identifying skills gaps the following should also be considered:
  - the use of **specialized tools**
  - **procedures** that are new to the individuals who will perform them
- These **gaps can result in risks** to the organization.

Criteria for "Yes" Response:

- *The organization **has identified the skill gaps** present in **all** cyber security personnel assigned to support the critical service.*
- *Or; the organization has determined there are **no skill gaps** present in **any** of the cyber security personnel assigned to support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has identified the skill gaps present in **some** cyber security personnel.*

4. Have training needs been identified? [OTA:SG3.SP1]

Question Intent: To determine if the organization has **identified training needs to address the identified skill gaps** of the personnel assigned to support the critical service (established in TA:G3.Q3).

- Training needs are established by analyzing the identified skill gaps and identifying the training needed to close those gaps.

CYBER RESILIENCE **ANALYSIS**

These are examples of sources to identify training needs:

- The roles and responsibilities of staff in the security, business continuity, and IT operations areas.
- The organization's vulnerability management process.
- The organization's service continuity process.
- The organization's compliance management process.
- The organization's incident management process.
- Training needs for external parties that may be supporting the critical service.

Criteria for "Yes" Response:

- *The organization **has identified the training needs** for **all** personnel assigned to support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has identified the training needs for **some** personnel.*

Goal 2 – Awareness and training activities are conducted.

1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]

Question Intent: To determine if **cyber security awareness activities** for the critical service **are conducted**.

- Awareness activities must meet the broad needs of staff members (established in TA:G1.Q1).
- The activities must be scheduled, advertised (if necessary), resourced, and tracked.

Typical work products include:

- awareness activity materials
  - newsletters
  - email campaigns
  - posters
  - presentations
- awareness activity schedules
- awareness activity logistics
- list of staff responsible for each awareness activity

Criteria for "Yes" Response:

- *The organization **has conducted cyber security awareness activities** for **all** personnel assigned to support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has conducted cyber security awareness activities for **some** personnel.*

2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]

Question Intent: To determine if **cyber security training activities** for the critical service **are conducted**.

- The organization must perform cyber security training to **ensure that staff is appropriately skilled** in their roles.
- Training should be **planned and scheduled.**

- Training provided should address identified skill gaps (established in TA:G1.Q3) including:
  - training in the use of **specialized tools**
  - training in **procedures** that are new to the individuals who will perform them

Typical work products include:

- delivered training courses
- training schedule

Criteria for "Yes" Response:

- *The organization **has conducted cyber security training activities** for **all cybersecurity personnel** assigned to support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has conducted cyber security training activities for **some** cybersecurity personnel.*

3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]

Question Intent: To determine if the effectiveness of the **cyber security awareness and training programs** for the critical service **is evaluated**.

- **A process should exist to determine the effectiveness** of the awareness and training programs in meeting the needs of staff that support the critical service.

Examples of methods to evaluate the effectiveness:

- testing on the presented material
- post-training surveys (e.g. instructor evaluation, manager feedback)
- focus groups
- selective interviews
- behavioral measures (password strength could be evaluated before and after a password-awareness activity.)
- observations, evaluations, and benchmarking activities

Criteria for "Yes" Response:

- *The organization has **evaluated the effectiveness of all** the cyber security **awareness and training programs** that support the critical service.*

Criteria for "Incomplete" Response:

- *The organization has evaluated the effectiveness of **some** of the cyber security awareness and training programs.*

4. Are awareness and training activities revised as needed? [OTA:SG1.SP3],[OTA:SG3.SP3]

Question Intent: To determine if the **awareness and training activities are revised** as needed.

- **Capabilities** for implementing the awareness and training plan **must be established and maintained**, including:
  - the selection of appropriate training approaches
  - sourcing or developing training materials
  - obtaining appropriate instructors
  - announcing the training schedule
  - revising the awareness and training capability as needed

CYBER RESILIENCE **ANALYSIS**

Situations in which awareness and training materials may need to be revised:

- training needs change (e.g., new technology is deployed)
- an evaluation of the training identifies the need for change
- changes in existing awareness needs and requirements
- emergence of new awareness needs and requirements
- assessments on the effectiveness of awareness and training activities (Established in TA:G2.Q3)
- training refresh

Criteria for "Yes" Response:

- *The organization revises, as needed, **all** of the cyber security **awareness and training activities** that are in support of the critical service.*

Criteria for "Incomplete" Response:

- *The organization revises, as needed, **some** of the cyber security awareness and training activities.*

5. Have privileged users been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]

Question Intent: To determine if **privileged users** have been **trained in their specific roles and responsibilities.**
NIST SP 800-53 Rev. 4 AT-3, PM-13:

- **Role-based security training is provided** to privileged users with assigned security roles and responsibilities:
  - **before authorizing their access** to the information system or before they perform their assigned duties
  - **when required** by information system changes
  - **periodically** (frequency defined by the organization) thereafter
- Comprehensive role-based training **addresses management, operational, and technical roles and responsibilities.**
- Role-based security training **also applies to contractors** providing services.

Criteria for "Yes" Response:

- ***All privileged users** that support the critical service **have been trained in their specific roles and responsibilities**.*

Criteria for "Incomplete" Response:

- ***Some** privileged users have been trained in their specific roles and responsibilities.*

6. Have senior executives been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]

Question Intent: To determine if **senior executives** have been **trained in their specific roles and responsibilities.**
NIST SP 800-53 Rev. 4 AT-3, PM-13:

- **Role-based security training is provided** to senior executives with assigned security roles and responsibilities:
  - **before authorizing their access** to the information system
  - **when required** by information system changes
  - **periodically** (frequency defined by the organization) thereafter
- Comprehensive role-based training **addresses management, operational, and technical roles and responsibilities.**

Criteria for "Yes" Response:

- ***All senior executives*** *that support the critical service* ***have been trained in their specific roles and responsibilities****.*

Criteria for "Incomplete" Response:

- ***Some*** *senior executives have been trained in their specific roles and responsibilities.*

7. Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]

Question Intent: To determine if **physical and information security personnel** have been **trained in their specific roles and responsibilities.**
NIST SP 800-53 Rev. 4 AT-3, PM-13:

- **Role-based security training is provided** to physical and information security personnel with assigned security roles and responsibilities:
  - **before authorizing their access** to the information system or before they perform their assigned duties
  - **when required** by information system changes
  - **periodically** (frequency defined by the organization) thereafter
- Comprehensive role-based training **addresses management, operational, and technical roles and responsibilities.**
- Role-based security training **also applies to contractors** providing services.

Criteria for "Yes" Response:

- ***All physical and information security personnel*** *that support the critical service* ***have been trained in their specific roles and responsibilities****.*

Criteria for "Incomplete" Response:

- ***Some*** *physical and information security personnel have been trained in their specific roles and responsibilities.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing training activities? [OTA:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** training activities **exists.**

- The plan defines training activities within the organization and **prescribes how training activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- training activities (developing awareness and training needs, evaluating gaps, training materials, conducting training, assessing effectiveness, etc.)
- standards and guidelines
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders

- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing training activities.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for training? [OTA:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** training activities **exists**.

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the training process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform training activities
- establishment of procedures, standards, and guidelines
- requirements for periodically assessing training effectiveness
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing training.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for training activities been identified and made aware of their roles? [OTA:GG2:GP7]

Question Intent: To determine if **stakeholders** for training activities have been **identified** and **made aware of their roles**.

Stakeholders of the training process have the following **responsibilities**:

- defining and managing training requirements
- conducting and overseeing the delivery of training
- ensuring the effectiveness of training

Examples of stakeholders include**:**

- critical service owners
- management
- training staff
- owners and custodians of assets that underpin the service
- critical service staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources
- internal and external auditors

Criteria for "Yes" Response:

- *__All__ stakeholders for the training activities have been __identified__ and __made aware__ of their roles.*

Criteria for "Incomplete" Response:

- *__Some__ stakeholders for the training activities have been __identified__ and __made aware__ of their roles.*
- *Or; stakeholders are identified but have __not been made aware__ of their roles.*

4. Have training standards and guidelines been identified and implemented? [OTA:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing training activities **have been implemented**.

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance of training activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- identifying awareness and training needs
- developing awareness and training plans
- developing awareness and training attendance requirements
- creating, delivering, and maintaining training material
- creating, delivering, and maintaining training records
- assessing the effectiveness of training and awareness programs

Criteria for "Yes" Response:

- *The organization has __implemented documented standards and guidelines__ for performing training activities.*

Criteria for "Incomplete" Response:

- *__Some__ standards and guidelines have been __implemented__.*

MIL3-Managed

1. Is there management oversight of the performance of the training activities? [OTA:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists**. The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the training activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the training activities.
- **Oversight** provides **visibility** into the training activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing or spot checks.

Examples of corrective actions:

- taking actions to update training materials to ensure effectiveness
- ensuring that standards and guidelines are followed
- adjusting resources (people, tools, etc.)

- identifying improvements in the training activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day training activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day training activities.*

2. Have qualified staff been assigned to perform training activities as planned? [OTA:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned.** The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan**.

- Qualified means that **staff are appropriately skilled** to perform training activities.

Examples of staff include personnel responsible for:

- designing, implementing, and assessing training
- implementing training processes, standards, and guidelines
- addressing issues and problems, including developing and executing remediation plans

Examples of skills needed include:

- curriculum and instructional design
- course delivery
- course and instructor evaluation
- measuring the effectiveness of awareness and training materials

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned training activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff** assigned have the skill necessary to perform their roles.*

3. Is there adequate funding to perform training activities as planned? [OTA:GG2.GP3.SP2],[GG2.GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided**. The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of training activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned training activities include**:**

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned training activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled? [OTA:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the training activities**.**

- The intent is to **determine risks that prevent the organization from performing training activities** (training process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the training process include:

- poorly defined training processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned training activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of* ***some*** *of the planned training activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of the planned training activities are* ***identified, but are not*** *analyzed, disposed of, monitored, or controlled.*

MIL4-Measured

1. Are training activities periodically reviewed and measured to ensure they are effective and producing intended results? [OTA:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To ensure the **training activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement.**

Periodic (as defined by the organization) reviews of the training process are needed to ensure that**:**

- awareness and training needs have been identified and are being satisfied
- training problem areas are identified and remediated
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risk related to training problem areas are identified and addressed
- actions requiring management involvement are elevated in a timely manner

CYBER RESILIENCE **ANALYSIS**

Example metrics of the training process may include:

- percentage of staff who have completed awareness training as required
- percentage of staff who have completed technical training as required
- percentage of favorable post-training evaluation ratings, including training effectiveness
- percentage of passing scores on training examinations

Criteria for "Yes" Response:

- ***All*** *training activities are* ***periodically*** *(as defined by the organization)* ***reviewed*** *and* ***measured*** *and the* ***results evaluated****.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review of the training activities.*
- *Or; review and measurement addresses* ***some*** *of the training activities.*
- *Or; training activities are* ***reviewed but not measured****.*

2. Are training activities periodically reviewed to ensure they are adhering to the plan? [OTA:GG2.GP8 & GP9],[GG2.GP8 & GP9]

Question Intent: To **periodically** determine if training activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the training plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing training activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- ***All*** *training activities are* ***periodically (as defined by the organization) reviewed*** *to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review.*
- *Or;* ***some*** *training activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to the performance of training? [OTA:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of training is **communicated** to higher level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher level managers include those in the organization **above the immediate level of management** responsible for the training process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

CYBER RESILIENCE **ANALYSIS**

Communication with higher level managers typically includes**:**

- **status** reviews of training activities
- **issues** identified in process and plan reviews
- **risks** associated with training activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher-level management is **made aware of issues** related to the performance of training through **scheduled** communication.*

Criteria for "Incomplete" Response:

- *The organization **has not established a frequency** for communication to higher-level management.*
- *Or; communications address **some** issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of training activities from which operating units can derive practices that fit their unique operating circumstances? [OTA:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines training.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in training activities across the organization.

A **standard definition** may include**:**

- process description
- process activities and practices to be performed
- process flow including diagrams
- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of training.*

Criteria for "Incomplete" Response:

- *A standard definition of training is **in development and partially documented**.*

2. Are improvements to training documented and shared across the organization? [OTA:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the training process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the training process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

CYBER RESILIENCE **ANALYSIS**

Examples of improvement work products may include**:**

- process metrics and measurements
- results of training effectiveness surveys
- course evaluations
- training records
- training requirements from a stakeholder group
- lessons learned from training plan reviews
- lessons learned in post-event reviews, including lack of staff preparedness

Criteria for "Yes" Response:

- ***Improvements*** *to training processes are* ***documented*** *and* ***shared*** *across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements*** *to training processes* ***are inconsistently documented****.*
- *Or;* ***not consistently shared*** *across the organization.*

CYBER RESILIENCE
ANALYSIS

10 Situational Awareness

The purpose of Situational Awareness is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.

Goals and Practices

Goal 1 – Threat monitoring is performed.

1. Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]

Question Intent: To determine if the **responsibility for monitoring sources of threat information** has been assigned. Effective threat monitoring requires the assignment of responsibility for threat monitoring activities.

- **Threat monitoring** is a process of data collection and distribution with the purpose of **providing timely, accurate, complete, and relevant** information about the organization's **current threat environment.**
- **Threat monitoring** is an integral part of establishing a common operating picture for the organization.

Responsible staff typically include:

- CISO office
- physical security
- technology administrators (i.e., network, server, database, etc.)
- asset owners

Example Sources:

- vendors' notifications
- industry groups (Internet Storm Center, Nextgov Threatwatch)
- international sources (multinational vendors, CERT-EU)
- weather alerts (NOAA)
- law enforcement (FBI InfraGard, IC3)
- DHS (ICS-CERT, US-CERT, sector-specific ISACs)

Criteria for "Yes" Response:

- ***The responsibility for*** *monitoring* ***all*** *sources of threat information relevant to the critical service* ***has been assigned****.*

Criteria for "Incomplete" Response:

- ***The responsibility for*** *monitoring* ***some*** *sources of threat information has been assigned.*

2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]

Question Intent: To determine if the organization has **implemented procedures** for monitoring threat information.

- **Effective monitoring requires** people, **procedures**, and technology that need to be deployed and managed to meet monitoring requirements.
- **Procedures ensure the timeliness, consistency, and accuracy** of threat information and the **distribution** of this information to relevant stakeholders.

Procedures may address:

- source identification
- monitoring frequency
- threat identification
- threat validation and analysis
- threat communication

Criteria for "Yes" Response:

- *The organization has **implemented** documented **procedures** for **all** threat monitoring activities relevant to the critical service.*

Criteria for "Incomplete" Response:

- *Procedures for **some** threat monitoring activities have been implemented.*

3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3]

Question Intent: To determine if resources have been **assigned and trained** to perform threat monitoring activities.

- The threat monitoring program must **take into consideration** the scope and breadth of the activities necessary to meet its goals, including **the human resources necessary** to fulfill requirements.
- Staff assigned to the monitoring process must have appropriate **knowledge of threat monitoring procedures.**
- **Training or skills improvement activities** must be conducted to meet threat monitoring requirements.

Examples of Training:

- operating, monitoring and configuring monitoring system components
- securing data collected from monitoring system components
- understanding and interpreting monitoring data
- communicating threat monitoring information to stakeholders

Criteria for "Yes" Response:

- ***Resources** have been **assigned and trained** to perform **all** threat monitoring activities relevant to the critical service.*

Criteria for "Incomplete" Response:

- *Resources have been assigned and trained to perform **some** threat monitoring activities.*
- *Or; resources have been **assigned but not trained**.*

Goal 2 – The requirements for communicating threat information are established.

1. Have internal stakeholders (such as the critical service owner and incident management staff) been identified to whom threat information must be communicated? [COMM:SG1.SP1]

Question Intent: To determine if **internal stakeholders** who must receive threat information **have been identified**.

- Internal stakeholders are identified to:
  - ensure communications about ongoing threat monitoring activities
  - promote threat awareness
  - ensure that the organization is performing under a common operating picture.

Examples of internal stakeholders include:

- members of the incident handling and management team
- asset owners and service owners
- information technology staff
- senior management
- business continuity staff
- human resources departments
- communications and public relations staff
- support functions such as legal and audit

Typical work products:

- list of internal stakeholders and alternates
- stakeholder contact information

Criteria for "Yes" Response:

- ***All internal stakeholders*** *who must receive threat information have been* ***identified and documented****.*

Criteria for "Incomplete" Response:

- ***Some*** *internal stakeholders have been identified and documented.*

2. Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated? [COMM:SG1.SP1]

Question Intent: To determine if **external stakeholders** who must receive threat information **have been identified**.

- External stakeholders are identified to
  - ensure communications about ongoing threat monitoring activities
  - promote threat awareness
  - ensure that the organization and its external stakeholders are performing under a common operating picture
- External stakeholders may have a stated role in communication plans or the service continuity plans of the organization.

Examples of external stakeholders include:

- first responders including law enforcement, fire, and medical
- media including newspaper, television, radio, and internet
- customers, business partners, and upstream suppliers
- local, state, and federal emergency management
- local utilities such as power, gas, telecommunications, and water
- legal, regulatory, and governing agencies

Typical work products:

- list of external stakeholders and alternates
- stakeholder contact information

Criteria for "Yes" Response:

- ***All external stakeholders*** *who must receive threat information have been* ***identified and documented****.*

Criteria for "Incomplete" Response:

- ***Some*** *external stakeholders have been identified and documented.*

Goal 3 – Threat information is communicated.

1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]

Question Intent: To determine if **threat information is communicated to** all identified **internal and external stakeholders**. The intent of communicating threat information is to ensure that the organization is operating under a common understanding of the threat environment.

- Threat information must be **communicated according to established requirements.**
- Communication requirements may dictate that various communications **methods and channels** should be considered and identified.
- The **infrastructure** to support those methods may need to be developed and implemented.

Example methods of communicating threat information include:

- threat communication standards and guidelines
- standardized report templates
- communication escalation protocols
- communication channels (email, text, mobile phone, etc.)

Typical work products:

- list of stakeholders and contact information
- stakeholder communication requirements
- documented methods and channels (by stakeholder class or requirement)
- tools and techniques for communication

Criteria for "Yes" Response:

- *Threat information is* ***communicated to all*** *identified* ***stakeholders*** *(established in SA:G2.Q1 and SA:G2.Q2) as required.*

Criteria for "Incomplete" Response:

- *Threat information is communicated to* ***some of the identified stakeholders****.*
- *Or;* ***some threat information*** *is communicated to all identified stakeholders.*

2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]

Question Intent: To determine if the **authority and accountability for communicating threat information** has been assigned. Effective threat communications requires the assignment of authority and accountability for threat communication activities.

- **Resources must be available** to meet threat communication requirements.
- The authority and accountability should be **detailed in job descriptions**.

Criteria for "Yes" Response:

- ***The authority and accountability for*** *communicating threat information* ***has been assigned*** *to* ***all*** *responsible resources.*

Criteria for "Incomplete" Response:

- ***The authority and accountability for*** *communicating threat information* ***has been assigned*** *to* ***some*** *of the responsible resources.*

3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]

Question Intent: To determine if the **resources** responsible for communicating threat information **have been trained** for their specific role.

- Training must be provided to staff that support and enable communications procedures.
- A skills inventory and gap analysis may be used to identify training requirements.

Typical work products:

- threat communication procedures with resources assigned
- job descriptions that contain threat communication responsibilities
- list of available and skilled resources
- list of skill and resource gaps
- training plan to address skill gaps

Criteria for "Yes" Response:

- ***All resources*** *assigned to perform threat communication activities have been* ***trained****.*

Criteria for "Incomplete" Response:

- ***Some*** *resources assigned to perform threat communication activities have been trained.*

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing situational awareness activities? [COMM:GG2.GP2],[MON:GG2.GP2],[GG2.GP2]

Question Intent: To determine if a **plan for performing** situational awareness activities **exists**.

- The plan defines situational awareness within the organization and **prescribes how situational awareness activities will be performed.**
- The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents.

The plan typically includes:

- situational awareness activities (monitoring threat sources, threat communication, etc.)
- standards and requirements
- roles, assignments of responsibility, resources, and funding
- identification of stakeholders

- measurement and reporting requirements
- training requirements
- management oversight

Criteria for "Yes" Response:

- *There is a **documented plan** for performing situational awareness.*

Criteria for "Incomplete" Response:

- *A plan is **in development and partially documented**.*

2. Is there a documented policy for situational awareness? [COMM:GG2:GP1.SP2],[MON:GG2:GP1.SP2],[GG2:GP1]

Question Intent: To determine if a **policy for performing** situational awareness activities **exists**.

- A **policy** is a written communication from the organization's senior management to employees.
- It **establishes the organizational expectations** for planning and performing the situational awareness process and **communicates those expectations** to the organization.

The policy should address:

- responsibility, authority, ownership, and the requirement to perform situational awareness activities
- establishment of procedures, standards, and guidelines
- approving threat communication methods and channels
- measuring adherence to policy, exceptions granted, and policy violations
- compliance with legal, regulatory, contractual, and government obligations

Criteria for "Yes" Response:

- *The organization has a **documented policy** for performing situational awareness.*

Criteria for "Incomplete" Response:

- *A policy is **in development and partially documented**.*

3. Have stakeholders for situational awareness activities been identified and made aware of their roles? [COMM:GG2:GP7],[MON:GG2:GP7]

Question Intent: To determine if **stakeholders** for situational awareness activities have been **identified** and **made aware of their roles**.

Stakeholders of the situational awareness process have the following **responsibilities**:

- identifying the threat monitoring and communication requirements
- defining and managing situational awareness activities, including ensuring the effectiveness of those activities
- overseeing the situational awareness process
- receiving and responding to threat information

Examples of stakeholders include:

- critical service owners
- management
- situational awareness staff
- owners and custodians of assets that underpin the service

- critical service staff
- service continuity staff
- external entities responsible for some part of the service
- information technology staff
- staff responsible for physical security
- human resources

Criteria for "Yes" Response:

- ***All*** *stakeholders for the situational awareness activities have been* ***identified*** *and* ***made aware*** *of their roles.*

Criteria for "Incomplete" Response:

- ***Some*** *stakeholders for the situational awareness activities have been* ***identified*** *and* ***made aware*** *of their roles.*
- *Or; stakeholders are identified but have* ***not been made aware*** *of their roles.*

4. Have situational awareness standards and guidelines been identified and implemented? [COMM:GG2.GP1],[MON:GG2.GP1]

Question Intent: To determine if **standards and guidelines** for performing situational awareness activities **have been implemented**.

- **Standards** establish expectations for performance.
- **Guidelines** are issued by an organization to ensure the **performance** of **situational awareness activities meets standards** and is **predictable, measurable,** and **repeatable.**

Standards and guidelines typically address:

- identifying threat monitoring requirements
- identifying threat communication requirements and protocols (e.g., who to call and when)
- identifying threat communication methods and channels
- communications with stakeholders based on their role
- collection and storage of threat data
- distribution of threat data

Criteria for "Yes" Response:

- *The organization has* ***implemented documented standards and guidelines*** *for performing situational awareness activities.*

Criteria for "Incomplete" Response:

- ***Some*** *standards and guidelines have been* ***implemented****.*

MIL3-Managed

1. Is there management oversight of the performance of situational awareness activities? [COMM:GG2.GP8],[MON:GG2.GP8],[GG2.GP8]

Question Intent: To determine if **management oversight exists**. The intent of **oversight** is to ensure the **direct day-to-day monitoring** of the situational awareness activities.

- **Management** consists of the immediate level of managers that govern the day-to-day operation of the situational awareness activities.

- **Oversight** provides **visibility** into the situational awareness activities so that **issues can be identified** and appropriate **corrective actions** can be taken when necessary.
- **Oversight activities** could include regular meetings, written or oral status updates, auditing, or spot checks.

Examples of corrective actions:

- taking actions to repair defective work products (monitoring procedures, communication procedures, sources of threat information, communication channels and methods) or services
- ensuring that standards and guidelines are followed
- ensuring training is conducted
- adjusting resources (people, tools, etc.)
- identifying improvements in the situational awareness activities
- escalating issues that require higher level management input for resolution

Criteria for "Yes" Response:

- *Management oversight of **all** the day-to-day situational awareness activities is being performed.*

Criteria for "Incomplete" Response:

- *Management oversight covers **some** aspects of the day-to-day situational awareness activities.*

2. Have qualified staff been assigned to perform situational awareness activities as planned? [COMM:GG2.GP3, GP4, & GP5],[MON:GG2.GP3, GP4, & GP5],[GG2.GP3, GP4, & GP5]

Question Intent: To determine if **qualified staff** have been **assigned**. The intent of this question is to **evaluate** the **qualifications** of the staff, **not the completeness of the plan**.

- Qualified means that **staff are appropriately skilled** to perform situational awareness activities.

Examples of staff include personnel responsible for:

- identifying the threat monitoring and communications requirements
- implementing processes, standards, and guidelines
- executing threat monitoring and communication processes
- addressing issues and problems, including developing and executing remediation plans

Examples of needed skills include:

- knowledge necessary to elicit and prioritize stakeholder requirements and interpret them to develop effective threat monitoring and communication requirements
- knowledge necessary to establish and maintain the threat monitoring and communications infrastructure
- knowledge necessary to interpret threat information and communicate it to stakeholders
- proficiency with tools, techniques, and methods used to perform threat monitoring and communications

Criteria for "Yes" Response:

- ***All staff** assigned to perform the planned situational awareness activities are **appropriately skilled**.*

Criteria for "Incomplete" Response:

- ***Some staff** assigned have the skill necessary to perform their roles.*

CYBER RESILIENCE **ANALYSIS**

3. Is there adequate funding to perform situational awareness activities as planned? [COMM:GG2.GP3.SP2],[MON:GG2.GP3.SP2],[GG2:GP3.SP2]

Question Intent: To determine if **adequate funding** has been **provided**. The intent of the question is to **evaluate** the completeness of the **funding**, **not the completeness of the plan**.

- **Funding** is an indication of higher level management support and sponsorship of situational awareness activities.
- **Funding** should be available to support the proper oversight, execution, and maintenance of these activities.

Considerations for funding planned situational awareness activities include**:**

- defining funding needs
- establishing a budget
- resolving funding gaps
- funding the process activities including staffing, tools, training, etc.

Criteria for "Yes" Response:

- ***Adequate funding*** *has been provided to perform* ***all*** *planned situational awareness activities.*

Criteria for "Incomplete" Response:

- *The planned activities have only been* ***partially funded****.*

4. Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled? [COMM:GG2.GP1],[MON:GG2.GP1],[RISK:SG1],[RISK:SG1.SP1]

Question Intent: To determine if the organization **identifies, analyzes,** and **mitigates risks related to the performance** of the situational awareness activities.

- The intent is to **determine risks that prevent the organization from performing situational awareness activities** (situational awareness process), not the risks to the organization if the activities are not performed.

Risks to consider in relation to the situational awareness process include:

- poorly defined situational awareness processes
- inadequate staffing
- inadequate funding
- unqualified staff
- lack of tools
- lack of a documented plan, policy, standards, and guidelines
- lack of stakeholder involvement
- lack of management oversight

Criteria for "Yes" Response:

- *Risks to the performance of* ***all*** *planned situational awareness activities are identified, analyzed, disposed of, monitored, and controlled.*

Criteria for "Incomplete" Response:

- *Risks to the performance of* ***some*** *of the planned situational awareness activities are identified, analyzed, disposed of, monitored, and controlled.*
- *Or; risks to the performance of planned situational awareness activities are* ***identified, but are not*** *analyzed, disposed of, monitored, or controlled.*

CYBER RESILIENCE ANALYSIS

MIL4-Measured

1. **Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results? [COMM:GG2.GP8 & GP9],[MON:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To ensure the **situational awareness activities (process) remain effective** and **produce intended results** by **periodic review** and **measurement**.
Periodic (as defined by the organization) reviews of the situational awareness process are needed to ensure that:

- threat sources are current and continue to be valid
- threat monitoring and communication requirements continue to be valid
- the infrastructure continues to adequately support requirements
- the quality of particular work products meets established guidelines
- problems in the process plan or in the execution of the process are identified
- risks related to situational awareness activities are identified and addressed
- actions requiring management involvement are elevated in a timely manner

Example metrics of the situational awareness process may include:

- uptime or availability of monitoring and communications infrastructure
- level of adherence to situational awareness process activities
- percentage of work products that do not meet standards
- percentage of stakeholders that do not receive communications
- time elapsed between the collection of key threat information and its distribution to stakeholders
- number of situational awareness requirements gaps
- number of new and changed situational awareness requirements over time

Criteria for "Yes" Response:

- ***All*** *situational awareness activities are* ***periodically*** *(as defined by the organization)* ***reviewed*** *and* ***measured*** *and the* ***results evaluated****.*

Criteria for "Incomplete" Response:

- *The organization* ***has not established a frequency*** *for review of the situational awareness activities.*
- *Or; review and measurement addresses* ***some*** *of the situational awareness activities.*
- *Or; situational awareness activities are* ***reviewed but not measured****.*

2. **Are situational awareness activities periodically reviewed to ensure they are adhering to the plan? [COMM:GG2.GP8 & GP9],[MON:GG2.GP8 & GP9],[GG2.GP8 & GP9]**

Question Intent: To **periodically** determine if situational awareness activities are being **performed as planned**.

- This review is often done by an independent entity (either internal or external to the organization).

Periodic (as defined by the organization) reviews for adherence to the situational awareness plan are needed to **ensure that:**

- Activities are **performed as planned and adhere to process descriptions, standards, and procedures.**
- Deviations from the plan are identified and evaluated.
- Problems in the plan for performing situational awareness activities are identified.
- Non-compliance is addressed.
- Needed process changes are identified when expected results or outputs are not met.

Criteria for "Yes" Response:

- *__All__ situational awareness activities are __periodically (as defined by the organization) reviewed__ to ensure that those activities are performed as planned.*

Criteria for "Incomplete" Response:

- *The organization __has not established a frequency__ for review.*
- *Or; __some__ situational awareness activities are reviewed to ensure that those activities are performed as planned.*

3. Is higher-level management aware of issues related to situational awareness? [COMM:GG2.GP10],[MON:GG2.GP10],[GG2.GP10]

Question Intent: To determine if the **performance** of situational awareness is **communicated** to higher level managers to **provide visibility** and **facilitate** the **resolution of issues**.

- Higher level managers include those in the organization **above the immediate level of management** responsible for the situational awareness process.
- **Communications** are expected to be **performed periodically** (as defined by the organization) and may be event-driven when escalation is needed.

Communication with higher level managers typically includes:

- **status** reviews of situational awareness activities
- **issues** identified in process and plan reviews
- **risks** associated with situational awareness activities
- **recommendations** for improvement

Criteria for "Yes" Response:

- *Higher level management is __made aware of issues__ related to the performance of situational awareness through __scheduled__ communication.*

Criteria for "Incomplete" Response:

- *The organization has __not established a frequency__ for communication to higher level management.*
- *Or; communications address __some__ issues.*

MIL5-Defined

1. Has the organization adopted a standard definition of the situational awareness activities from which operating units can derive practices that fit their unique operating circumstances? [COMM:GG3.GP1],[MON:GG3.GP1],[GG3.GP1]

Question Intent: To determine if the organization has a **standard process** that defines situational awareness.

- A **standard process** should include **guidelines for tailoring** the process to meet the needs of an organizational unit.
- A standard process **provides a predictable level of consistency** in situational awareness activities across the organization.

A **standard definition** may include:

- process description
- process activities and practices to be performed
- process flow including diagrams

- inputs and expected outputs
- performance measures for improvement
- procedures for process improvement

Criteria for "Yes" Response:

- *The organization has **adopted a standard definition** of situational awareness.*

Criteria for "Incomplete" Response:

- *A standard definition of situational awareness is **in development and partially documented**.*

2. Are improvements to situational awareness activities documented and shared across the organization? [COMM:GG3.GP2],[MON:GG3.GP2],[GG3.GP2]

Question Intent: To ensure that **improvements** to the situational awareness process are **documented** and **shared** across the organization.

- **Documenting lessons learned** during the execution and review of the situational awareness process facilitates the proposal of improvements to the process.
- **Sharing lessons learned** enables organization-wide process improvements and organization-wide learning.

Examples of improvement work products may include:

- process metrics and measurements
- direct feedback from stakeholders
- lessons learned in post-event review of incidents and disruptions in continuity
- lessons learned from periodic reviews of situational awareness activities that can be applied to improve the situational awareness process
- risk evaluations

Criteria for "Yes" Response:

- ***Improvements** to situational awareness processes are **documented** and **shared** across the organization.*

Criteria for "Incomplete" Response:

- ***Improvements** to situational awareness processes **are inconsistently documented**.*
- *Or; **not consistently shared** across the organization.*