Cyber Resilience Review (CRR): Question Set with Guidance

February 2014

Homeland Security

Copyright 2014 Carnegie Mellon University

The Cyber Resilience Review is based on the Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM), both developed at Carnegie Mellon University's Software Engineering Institute. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, pursuant to the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in Federal Government Contract Number FA8721-05-C-0003 with the Software Engineering Institute.

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

NO WARRANTY

ANY MATERIAL OF CARNEGIE MELLON UNIVERSITY AND/OR ITS SOFTWARE ENGINEERING INSTITUTE CONTAINED HEREIN IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

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

External Use: Additionally, this material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Permission can be obtained at http://www.sei.cmu.edu/legal/permission/crr.cfm.

Table of Contents

1 Asset Management **1**
Goals and Practices 1
Maturity Indicator Levels 8
2 Controls Management **12**
Goals and Practices 12
Maturity Indicator Levels 14
3 Configuration and Change Management **18**
Goals and Practices 18
Maturity Indicator Levels 21
4 Vulnerability Management **25**
Goals and Practices 25
Maturity Indicator Levels 30
5 Incident Management **33**
Goals and Practices 33
Maturity Indicator Levels 39
6 Service Continuity Management **43**
Goals and Practices 43
Maturity Indicator Levels 47
7 Risk Management **51**
Goals and Practices 51
Maturity Indicator Levels 55
8 External Dependencies Management **59**
Goals and Practices 59
Maturity Indicator Levels 64
9 Training and Awareness **68**
Goals and Practices 68
Maturity Indicator Levels 71
10 Situational Awareness **74**
Goals and Practices 74
Maturity Indicator Levels 76

1 Asset Management

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

Goals and Practices

Goal 1 – Services are identified and prioritized.

1. Is the organizations mission, vision, values and purpose, including the organizations place in critical infrastructure, identified and communicated? [EF:SG1.SP1]

Strategic objectives are the performance targets that the organization sets to accomplish its mission, vision, values, and purpose.

General objectives include mission, vision, and values, while specific objectives are goal oriented and outline the targets the organization is attempting to reach. For example:

- Opening 100 stores
- Improving revenue by 14%

This information may be readily available in company literature such as employee handbooks and annual reports.

Resilience activities must meet strategic objectives by protecting and sustaining assets and services to the extent necessary to attain these objectives.

Typical work products:

1. Organizational strategic objectives
2. Organizational mission, vision, values, and purpose statement

A yes answer means that the organization has documented and communicated the organization's mission including the organization's place in critical infrastructure.

2. Are the organization's mission objectives and activities prioritized? [EF:SG1.SP3]

The high-value services of the organization directly support the achievement of strategic objectives and therefore must be protected and sustained to the extent necessary to minimize disruption. The high-value services of the organization must be identified, prioritized, and communicated as a common target for success.

Analyzing organizational services in relation to strategic objectives is a means to help the organization prioritize services and to identify high-value services that must be made resilient.

Typical work products

- Prioritized list of organizational mission objectives
- Service and mission objective analysis
- Prioritized list of associated services

A yes answer means that the organizations mission objectives and activities are prioritized.

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

A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. Identifying services, their associated assets, and the activities that support these services must be performed before the organization attempts to develop service continuity plans.

A yes answer means that the organization has documented its services as a part of an established business process, and the current list of services is accurate.

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

Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to high-value services are identified and analyzed in risk assessment activities. The organization must consider this information when prioritizing high-value services. Typical work products include:

1. Prioritized list of organizational services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

A yes answer means that the identified services include a priority, or that there is a separate repository of information that prioritizes services based on their potential impact of disruption.

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? [ADM:SG1.SP1]

Organizations may use many practical methods to inventory these assets. Human resources databases identify and describe the roles of vital staff. Fixed asset catalogs often describe all levels of technology components. Facilities and real estate databases have information about high-value physical plant assets. However, bear in mind that internal databases may not cover people, technology, and facilities that are not under the direct control of the organization. In contrast to people, technology, and facilities, less tangible assets such as information and intellectual property may not be identified and regularly inventoried because they are often difficult to describe and bound. For example, a staff member may have information that is critical to the effective operation of a service that has not been documented or is not known to other staff members. This must be resolved in order to properly define security and continuity requirements for these assets.

A yes answer means that the organization has documented in one or more repositories the people, information, technologies, and facilities essential to the operation of the critical service, and that documentation is current.

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

An organization may document the asset's protection and sustainment requirements as part of the asset profile so that there is a common source for communicating and updating these requirements and so that their association with an asset is established. In addition, strategies to protect and sustain an asset may be documented as part of the asset profile.

A yes answer means that the organization includes protection and sustainment requirements as a part of its asset's descriptions in inventories, and the current documented requirements are accurate.

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

Asset custodians are persons or organizational units, internal or external to the organization, who are responsible for implementing and managing controls to satisfy the resilience requirements of high-value assets while they are in their care. For example, the customer data in the above example may be stored on a server which is maintained by the IT department. In essence, the IT department takes custodial control of the customer data asset when the asset is in its domain. The IT department must commit to taking actions commensurate with satisfying the owner's requirements to protect and sustain the asset. However, in all cases, owners are responsible for ensuring that their assets are properly protected and sustained, regardless of the actions (or inactions) of custodians.

The owner of each high-value asset is established in order to define responsibility and accountability for the asset's resilience and its contributions to services. Accordingly, owners are responsible for developing and validating the resilience requirements for high-value assets that they own. They are also responsible for the implementation of proper controls to meet resilience requirements, even if they assign this responsibility to a custodian of the asset.

A yes answer means that the organization includes asset owners and custodians as a part of asset descriptions in inventories, and that information is current.

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

At a minimum, all high-value assets should be defined to the extent possible. Differences in the level of description are expected from asset to asset, and an organization must decide how much information is useful in facilitating requirements definition and satisfaction. There are some common elements that should be collected, at a minimum, for each asset. Important information includes the physical location of the asset. These are examples of information that should be collected and documented for assets:

- Asset type (people, information, technology, or facilities)
- Categorization of asset by sensitivity (generally for information assets only)
- Asset location (typically where the custodian is managing the asset)
- Asset owners and custodians
- The format or form of the asset
- Location where backups or duplicates of this asset exist (particularly for information assets)
- The services that are dependent on the asset
- The value of the asset in either qualitative or quantitative terms

A yes answer means that the organization includes physical location as a part of asset descriptions in inventories, and that information is current.

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]

To provide a service-focused review of operational resilience, the assets collected in the development of the asset inventory must be associated with the services they support. This helps the organization view resilience from a service perspective and to identify critical dependencies that are essential to determining effective strategies for protecting and sustaining assets.

A yes answer means that the organization includes documentation of the services that assets support in inventories, and that information is current.

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

The needs of the organization and the protection and continuity requirements of services are translated into asset-level resilience requirements. In practical application, this requires three distinct activities:

- Identification of high-value services. High-value services are those on which the success of the organization's mission is dependent.
- Identification and association of assets to organizationally high-value services. Mission assurance of services relies on the consistent and effective productivity of related assets—people, technology, information, and facilities. The needs of the service in meeting its mission guide the development of asset-level resilience requirements.
- Development of asset-level requirements based on the asset's deployment in, contributions to, and support of associated services.

Because of the association between services and assets, the resilience requirements of a service are essentially represented by the collective resilience requirements of associated assets.

A yes answer means that the organization has documented confidentiality, integrity, and availability requirements for its assets, and that information is current.

Goal 4 – The asset inventory is managed.

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

In order to identify changes to high-value assets that could affect their productivity and resilience, the organization must have a set of criteria that are consistently applied. These criteria must cover all assets—people, technology, information, and facilities. Changes in assets must be translated to changes in resilience requirements—either the requirements are altered or rewritten, or in the case where the asset is eliminated (for example, when vital staff leave the organization), the requirements are retired.

These are examples of triggers that can affect high-value assets:

- Changes in organizational structure and staff—termination or transfer of staff between organizational units or changes in roles and responsibilities
- Changes in technology infrastructure and configuration
- Real-estate transactions that add, alter, or change existing facilities
- Creation or alteration of information
- Changes in services affecting the assets on which they rely
- Contracts that the organization enters into that would identify new assets
- Acquisition of assets such as technology or facilities

A yes answer means that the organization has documented change criteria requirements for its assets, and that information is current.

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

This practice also addresses changes to the description or composition of an asset. For example, if an asset takes an additional form (such as when a paper asset is imaged or an electronic asset is printed), this must be documented as part of the asset description to ensure that current strategies to protect and sustain align properly and provide coverage across a range of asset media. Assets may also change ownership, custodianship, location, or value—all of which must be updated to ensure a current asset profile and inventory.

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.

A yes answer means that the organization can trace asset description updates to scheduled and approved changes.

Goal 5 – Access to assets is managed.

1. Is access to assets granted based on their protection requirements? [AM:SG1.SP1]

Access should be granted in accordance with the justification for the request and the protection requirements that have been established for the asset. Asset owners are responsible for reviewing the request, justification, and 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 possible, the approval for the access should be limited to a specific time period (one week, one month, one year), to prevent the privilege from extending beyond the requestor's need.

If the custodian of the asset is different from the owner, the owner should communicate in writing the approval for the request.

A yes answer means that the organization has identified the protection requirements for assets, and uses those as a basis to grant or deny access privileges.

2. Are access requests reviewed and approved by the asset owner? [AM:SG1.SP1]

Access should be granted in accordance with the justification for the request and the resilience requirements that have been established for the asset. Asset owners are responsible for reviewing the request, justification, and resilience 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 possible, the approval for the access should be limited to a specific time period (one week, one month, one year), to prevent the privilege from extending beyond the requestor's need. Limiting the term of the approval also provides the asset owner a chance to review privileges when they come up for renewal and to make changes if necessary.

If the custodian of the asset is different from the owner, the owner should communicate in writing their approval for the request as well as any modifications of the request that they deem appropriate given their review. Access requests should not be forwarded to custodians for implementation unless they have been approved by asset owners.

If an asset owner decides to extend access rights that exceed stated resilience requirements or extend beyond the need established by the requestor's job responsibilities, the owner should document this decision and identify any potential risk that may occur as a result. Risks should be addressed through the organization's formal risk management process.

A yes answer means that asset owners review and approve access requests. Ideally, this approval is documented.

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

Periodic review of access rights is the primary responsibility of the owners of organizational assets. They must ensure that the requirements they have set for their assets are being implemented through proper assignment of access privileges and implementation of corresponding access controls. Owners are also responsible for taking action whenever access rights do not correspond with legitimate identity needs and existing resilience requirements.

During periodic review, there are two particular problems that owners of assets should be attuned to:

- The first is misalignment between existing access privileges and the resilience requirements established for the assets. In this case, access privileges that have been provisioned to identities violate the resilience requirements that owners have set for the assets.
- The second is misalignment between existing access privileges and the roles and job responsibilities of the identities that possess the privileges. In this case, there is no violation of the resilience requirements, but privileges that are more extensive than necessary have been provisioned to identities that do not require this level of access.

A yes answer means that the organization periodically reviews access privileges to ensure they are appropriate. This review should be documented and current.

4. Are access privileges modified as a result of reviews? [AM:SG1.SP3]

A disposition for each inconsistency or misalignment should be documented, as well as the actions that need to be taken to correct these issues

A yes answer means that the organization periodically reviews access privileges to ensure they are appropriate. This review should be documented and current. Changes to access privileges that arise from reviews should be documented.

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]

The categorization of information assets is a key consideration in the development of adequate resilience requirements and in the implementation of strategies to protect and sustain them.

An information sensitivity categorization scheme and corresponding information handling processes and procedures provide a way for the organization to put its mark on information assets relative to their risk tolerances and to allow for an appropriate level of corresponding handling, protection, and resilience. Failure to provide an information sensitivity categorization scheme allows for organizational staff to determine sensitivity using their own guidelines and judgment, which may vary widely. A consistently applied sensitivity categorization scheme also ensures consistent handling of information assets across the organization and with external business partners.

A yes answer means that the organization has developed (and uses) categories for the classification of information based on sensitivity to the critical service.

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

Monitor the effectiveness of the categorization of information assets, and identify deficiencies that must be resolved.

A yes answer means that the organization provides oversight, such as audits or spot-check inspections to ensure that the approved methods of information categorization are being followed.

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

The sensitivity categorization scheme is unique to the organization and should cover all categories of information assets. The categorization levels should be appropriately defined and communicated and integrated with information asset handling and labeling procedures.

A yes answer means that the organization has policies and procedures available that instruct employees on how to categorize and manage information.

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]

Administrative controls for protecting information assets include training to ensure proper information asset definition and handling.

A yes answer means that the organization instructs staff on the approved methods of categorizing information.

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

The duplication and retention of information assets are primary controls for ensuring information asset availability. These controls must be applied not only to information assets that are critical to supporting high-value services but also to the restoration of these services when disrupted.

A yes answer means that the organization's high-value information assets are backed-up and retained?

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

The controlled disposition of information assets is necessary to ensure that they are not disclosed to unauthorized staff. As an information asset is retired from service, it must be disposed of in a manner commensurate with its resilience requirements and sensitivity categorization, and in accordance with any applicable rules, laws, and regulations.

A yes answer means that the organization has policies and procedures available that instruct employees on how to dispose of information assets.

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

Proper disposition of information assets is highly dependent on the type of asset, its form, its sensitivity categorization, and other factors such as whether the disposition must be logged or tracked. The organization must develop specific guidelines to address a range of disposition issues and address them through provision of proper disposition methods such as the use of shredders or incineration.

A yes answer means that the organization provides oversight, such as audits or spot-check inspections to ensure that the approved methods of information disposal are being followed.

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]

Facility asset prioritization is performed relative to related services—that is, facility assets associated with high-value services are those that must be most highly prioritized for operational resilience activities. However, the organization can use other criteria to establish high-priority facility assets, such as the following:

- The use of the facility asset in the general management and control of the organization (corporate headquarters, primary data centers, etc.)
- Facility assets that are important to supporting more than one service
- The value of the asset in directly supporting the organization's achievement of critical success factors and strategic objectives
- The organization's tolerance for "pain"—the degree to which it can suffer a loss or destruction of the facility asset and continue to meet its mission.

A yes answer means that the organization has a procedure to prioritize facilities based on impact, and that prioritized list is available and current.

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

Periodically validate and update the list of high-value facility assets based on operational and organizational environment changes.

A yes answer means that the organization reviews the prioritized list of facility assets and reaffirms the priority. This review should be documented and current.

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

A specific subset of controls should be considered during the design, construction, or leasing of facility assets. These controls are typically technical or physical in nature and are focused on sustaining the operability and viability of facilities, thus contributing to a facility's operational resilience.

A yes answer means that the organization reviews resilience requirements for the services that will be conducted in the facility assets, and ensures that the requirements will be met.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing asset management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes
- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for asset management?

A policy is a written communication from the organization's senior management to employees.

The policy should address:
- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines

- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for asset management activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities.

Examples of stakeholders include:
- Critical service owners
- Owners and custodians of assets
- 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

4. Have asset management standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the asset management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform asset management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:
- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform asset management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process. Funding the process can include
- Defining funding needs

- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are asset management activities periodically reviewed to ensure they are adhering to the plan?

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

For example, the review can include

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of asset management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers.

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to asset management activities documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

Control objectives are broad-based targets for the effective and efficient performance of controls. Establishing control objectives is an activity that guides the organization's ability to link controls to management directives

Typical work products:

- Management directives and guidelines for selecting control objectives
- Control objectives
- Criteria for prioritizing control objectives
- List of prioritized control objectives

A yes answer means that the organization has documented control objectives for all asset types that support the critical service (people, information, technology, and facilities), and the documents are current.

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

The intent of prioritization is to determine the control objectives that most need attention because of their potential to affect the critical service. Assigning a relative priority to each control objective or category aids in determining the level of resources to apply when defining, analyzing, assessing, and addressing gaps in controls. Management directives and guidelines can be used to establish criteria for prioritizing control objectives.

A yes answer means that the organization has prioritized its established control objectives. This prioritization should be documented and current.

Goal 2 – Controls are implemented.

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

Administrative, technical, and physical controls are established to meet operational resilience management control objectives. Controls can be at the enterprise level or at the service and asset level.

A yes answer means that the organization has identified contol objectives for assets that support the critical service, and has implemented controls that are intended to achieve those objectives.

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]

Analysis of controls is focused on ensuring that controls (both existing and proposed) meet one or more control objectives and, by extension, resilience requirements. Analysis also ensures that all service-level control objectives are adequately satisfied by one or more service-level controls and asset-level controls for assets that support the service. Analysis may range from a subjective review of the control's ability to meet the control objective to the development and execution of tests that demonstrate the control's capability. The organization must determine the level of analysis necessary in each case; however, the importance of the control in supporting operational resilience should determine the extent of analysis required and which analysis techniques are deployed.

Controls analysis should also help the organization to identify:

- Any gaps where the control does not fully meet one or more control objectives
- Any gaps where an enterprise-level control objective that addresses the resilience of services and supporting assets is not adequately satisfied by one or more controls
- Any gaps where a service control objective is not adequately satisfied by one or more service- or asset-level controls

Typical work products:

- Analysis results
- Control objectives that are satisfied by controls
- Updated traceability matrix of control objectives and the controls that satisfy them
- Control gaps
- Updates to existing controls
- Proposed new controls
- Risks related to unsatisfied control objectives
- Risks related to redundant and conflicting controls

A yes answer means that the organization has identified control objectives for assets that support the critical service, and identifies gaps where existing controls do not meet the objectives.

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

Additional updates to existing controls and proposed new (perhaps combined) controls are identified to resolve these issues. This includes identifying gaps where the control objective's priority does not warrant further investment in updated or new controls.

A yes answer means that the organization analyses its controls to ensure that they meet determined control objectives, and the results of that analysis is to modify existing controls or introduce new controls.

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]

Performing periodic assessment of the internal control system is necessary to ensure that controls continue to meet control objectives, that control objectives continue to implement strategies for protecting and sustaining services (and their supporting assets), and that resilience requirements are satisfied. Conversely, assessment of the internal control system identifies areas where controls are ineffective and inefficient along with

determining whether controls need to be modified to reflect changing business and risk conditions. Controls assessment provides opportunities to save cost by eliminating redundant controls and resolving control conflicts.

Typical work products:

- Assessment scope
- Assessment results
- Problem areas
- Updates to existing controls
- Proposed new controls
- Remediation plans
- Updates to service continuity plans
- Risks related to unresolved problems

A yes answer means that the organization periodically assesses the performance of controls to ensure that they continue to meet there control objectives. This review should be documented and current per the organization's schedule.

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

As a result of conducting the assessment process, the organization may learn of areas that need attention, particularly if they are keeping the organization from meeting business objectives or compliance obligations. These areas may require the creation of detailed remediation plans and strategies to ensure that control objectives are sufficiently achieved by controls.

A yes answer means that and the results of assessments are used to modify existing controls or introduce new controls.

Maturity Indicator Levels

MIL2-Planned

1. Is there a plan for performing controls management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for controls management?

A policy is a written communication from the organization’s senior management to employees.

The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines

- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for controls management activities have been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities.

Examples of stakeholders include
- Critical service owners
- Owners and custodians of assets
- 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

4. Have controls management standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the controls management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform controls management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:
- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform controls management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process.

Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are controls management activities periodically reviewed to ensure they are adhering to the plan?

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

For example, the review can include

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of controls management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers.

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to controls management documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

Organizational and operational conditions are continually changing. These changes result in daily changes to the high-value assets that help the organization's services achieve their missions.

Besides the addition of new assets, this practice also addresses changes to the description or composition of an asset. For example, if an asset takes an additional form (such as when a paper asset is imaged or an electronic asset is printed), this must be documented as part of the asset description to ensure that current strategies to protect and sustain align properly and provide coverage across a range of asset media. Assets may also change ownership, custodianship, location, or value—all of which must be updated to ensure a current asset profile and inventory.

In addition, whenever assets are eliminated (for example, a server is retired or vital staff members leave the organization), owners of those assets must ensure that their resilience requirements are either eliminated (if possible) or are transferred and updated to the assets that replace them. Doing this is especially critical when assets are shared between services and have common resilience requirements.

A yes answer means that the organization has a process to control changes to assets that support the critical service, and that process is used by all relevant staff.

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

Change management for resilience requirements is a continuous process and therefore requires that the organization effectively assign responsibility and accountability for it. The organization must independently monitor that the change management process is operational and that asset-level resilience requirements have been updated on a regular basis so that they remain in direct alignment with organizational drivers. In most cases, these responsibilities will fall to asset owners as part of their management of the assets over their life cycles.

A yes answer means that the organization reviews resilience requirements as a part of the change management process to ensure that strategies to protect and sustain assets align with organizational needs.

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

Capacity is a significant factor in meeting the availability requirements of technology assets and in turn of the services that rely on these assets. The operating capacity of technology assets must be managed commensurate with operational demands to support services; otherwise these services will be affected by diminished operability and potentially fail to meet their missions.

Capacity planning and management involves measurement of current demand, tests for anticipated demand, and gathering usage trends over time to be able to predict expansion needs. Consideration of capacity to

ensure technology availability and meet business objectives requires a pro-active approach to managing demand and anticipating future needs.

Typical work products include:

1. Capacity management strategy
2. Capacity forecasts
3. Capacity statistics and performance metrics

A yes answer means that the organization manages the capacity of its technology assets, and capacity is measured using identified metrics.

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

Ensure that all change requests have a disposition and that changes that have not been closed are provided an updated status.

A yes answer means that the organization manages changes to its assets, and change requests are monitored until they are resolved.

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

The organization should establish communication channels to ensure custodians are aware of changes in assets, and update service level agreements with custodians if necessary to reflect commitment to changes.

A yes answer means that the organization notifies stakeholders of changes to assets, and that process is used for all changes.

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

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

Configuration management is a fundamental resilience activity. It supports the integrity of technology assets by ensuring that they can be restored to an acceptable form when necessary (perhaps after a disruption) and provides a level of control over changes that can potentially disrupt the asset's support to organizational services. When integrity is suspect for any reason, the resilience of technology assets and associated services may be affected.

A yes answer means that the organization performs configuration management for its technology assets.

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

An important component of configuration management is the ability to control and manage changes to technology assets, particularly to configuration items. Because of the nature of the operational environment, most technology assets are expected to change over time; the addition of new functionality, repair of software bugs and security vulnerabilities, or the retirement or replacement of hardware components means that changes will alter the original configuration of the asset. Defining and communicating change procedures, including both routine and emergency changes, ensures that changes to technology assets will be handled in an efficient and controlled manner, consistent with organizational policy, standards, and guidelines, with minimum impact to the integrity, availability, and ultimately the resilience of the asset and the services it supports.

Change control and management defines an organizational process that introduces structure and rigor to making changes to technology assets and provides a means for tracking these changes so that problems can be detected and remedied. This provides an enhanced level of confidence in the integrity of the technology asset and its ability to perform its intended function.

A yes answer means that the organization has implemented methods to discover changes to technology assets. These methods may be administrative (policies, procedures), technical (change management software) or physical (inspection, audit).

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

Regularly audit the integrity of the configuration item baselines to ensure that they are complete and correct and that they continue to meet configuration management standards and procedures. Identify action items that are required to repair any anomalies.

A yes answer means that the organization regularly reviews modifications to technology assets to ensure that they are following the standard procedure.

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

Controlling modification of information assets by authorized staff ensures the continued integrity of these assets. A fundamental way of controlling modification is to control access to these information assets, both electronically (via controlling access to networks, servers, application systems, and databases and files) and physically (by limiting access to file rooms, work areas, and facilities).

A yes answer means that the organization considers which staff members have authorization to make modifications to information assets, based on the unique integrity requirements of each information asset, and implements controls to meet these requirements.

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

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.

A yes answer means that the organization has implemented controls to identify and analyze the modifications of information assets as they are used by the critical service.

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

Periodically verify (through monitoring and auditing) that changes to configurations are valid and authorized.

A yes answer means that the organization monitors for unauthorized changes to technology assets, and works to ensure that no unauthorized changes exist within the technical infrastructure.

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

To minimize operational impact, the organization must test the release build in a segregated test environment to identify issues, concerns, and problems that may cascade into other operational areas when the build is released. Once all operational issues have been defined and addressed (in some cases by “rebuilding” the build), the organization can proceed to move the release build into the production environment.

A yes answer means that the organization tests changes to technology assets before they are released to production.

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

Controlled 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, controlling the access to utility programs may prevent changes to a technical asset's baseline configuration. On the other hand, ensuring that a server is placed behind a physically protected barrier or in a secure room is a physical access control that may prevent destruction of the server or the ability to manipulate configuration settings directly from a console. For software technology assets (and in some cases, firmware), access controls tend to be electronic; for hardware technology assets, access controls can be electronic or physical.

A yes answer means that a process for controlling access to high-value technology assets is documented and current.

Goal 3 – Asset configuration baselines are established.

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

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 life cycle. Configuration management also establishes additional controls over the asset so that it is always in a form that is available and authorized for use. In some cases, an organization may want to freeze a baseline technology asset configuration, thus permitting no modifications or alterations to the asset over its life cycle.

A yes answer means that the organization has developed configuration standards for technology assets, and ensures that those baselines are adhered to.

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

An important component of configuration management is the ability to control and manage changes to technology assets, particularly to configuration items. Because of the nature of the operational environment, most technology assets are expected to change over time; the addition of new functionality, repair of software bugs and security vulnerabilities, or the retirement or replacement of hardware components means that changes will alter the original configuration of the asset. Defining and communicating change procedures, including both routine and emergency changes, ensures that changes to technology assets will be handled in an efficient and controlled manner, consistent with organizational policy, standards, and guidelines, with minimum impact to the integrity, availability, and ultimately the resilience of the asset and the services it supports.

A yes answer means that the organization ensures approval of modifications to technology asset baseline configurations.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing change management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for change management?

A policy is a written communication from the organization's senior management to employees.

The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for change management activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities.

Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have change management standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the change management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform change management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform change management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process.

Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are change management activities periodically reviewed to ensure they are adhering to the plan?

This review is often done by an independent entity (either internal or external to the organization). For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned

- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of change management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers.

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include:
- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to change management documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

The strategy for addressing vulnerability analysis and resolution should be documented in a plan that can be communicated to relevant stakeholders and implemented. The plan should address:

- The scope of vulnerability analysis and resolution activities
- The essential activities that are required for vulnerability analysis and resolution
- A plan for collecting the data necessary for vulnerability activities
- Tools, techniques, and methods that have been approved for identifying and analyzing vulnerabilities across a range of assets
- A schedule for performing vulnerability activities
- The roles and responsibilities necessary to carry out the plan
- The skills and training required to perform the vulnerability analysis and resolution strategy and plan
- The relative costs associated with the activities, particularly for the purchase and licensing of tools, techniques, and methods
- Relevant stakeholders of the vulnerability activities and their roles
- Objectives for measuring when the plan and strategy are successful

A yes answer means that a strategy for addressing vulnerability analysis and resolution is documented and influences plans and procedures.

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

The organization should compile a list of approved and recommended tools, techniques, and methods that can be used for vulnerability activities. Pre-approving tools, techniques, and methods ensures consistency and cost-effectiveness, as well as validity of results. This list should cover the entire range of assets and include both procedural and automated methods.

A yes answer means that a list has been compiled. An answer of incomplete means that a list is being developed. A no answer means that the task has not been performed.

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

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

Information about potential vulnerabilities is available from a wide variety of organizational and external sources. External or public sources typically provide information that is focused on common technologies that are used by a wide range of organizations. Internal sources typically provide information about vulnerabilities that are unique to the organization and range across all types of assets, including people, information, and

facilities. Internal sources of vulnerability information are often generated by other operational resilience management processes such as incident management and monitoring, or through IT service delivery and operations processes such as the service desk and problem management. These sources may provide information about vulnerabilities that the organization has observed or that have been exploited, resulting in disruption to the organization.

These are examples of sources of vulnerability data:

- Vendors of software, systems, and hardware technologies who provide warnings on vulnerabilities in their products
- Common free catalogs, such as the US-CERT Vulnerability Notes Database and The MITRE Corporation's Common Vulnerabilities and Exposures List
- Industry groups
- Vulnerability news groups and mailing lists
- The results of executing automated tools, techniques, and methods
- Internal processes such as service desk, problem management, incident management and control, and monitoring, where vulnerabilities may be detected

A yes answer means that sources of vulnerability information have been identified and documented.

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

Vulnerability data collection is a continuous process. Expanding the sources of vulnerability information helps the organization improve its identification of vulnerabilities in a timely manner and extends the organization's awareness of an expanding range of vulnerability types. The organization must ensure that as new vulnerability information sources become available they are incorporated into the organization's vulnerability repository and corresponding identification and analysis activities.

New sources of vulnerability information are continually emerging. The organization must review these sources and add them to its source list to be sure to have access to the most current, accurate, and extensive information about vulnerabilities.

A yes answer means that information from the sources are regularly reviewed and updated as necessary.

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

Vulnerabilities are discovered from active review and capture from the organization's standard list of sources of vulnerability information. There are many techniques that an enterprise can use to discover vulnerabilities. These include:

- Performing internal vulnerability audits or assessments (using tools, techniques, and methods)
- Performing external-entity assessments
- Reviewing the results of internal and external audits
- Periodically reviewing vulnerability catalogs, such as the US-CERT
- Vulnerability Notes Database and The MITRE Corporation's Common Vulnerabilities and Exposures List
- Subscribing to vendor notification services
- Subscribing to vulnerability notification services (mailing lists)
- Reviewing reports from industry groups
- Reviewing vulnerability news groups
- Using lessons-learned databases, such as the incident knowledge base (The incident knowledge base is addressed in the Incident Management and Control process area.)
- Monitoring high-value organizational processes and infrastructure (Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.)

- Using reports of vulnerabilities from other process such as the organization's service desk or the problem management process

A yes answer means that the organization performs regular activities to learn about vulnerabilities throughout its assets (people, information, technology, facilities) and processes.

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

Based on the organization's prioritization guidelines and the results of vulnerability analysis, vulnerabilities must be categorized by disposition.

These are examples of categories for vulnerability resolution:

- Take no action; ignore
- Fix immediately (typically the case for vendor updates or changes)
- Develop and implement 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

Vulnerabilities that are referred to the risk management process are typically those that cannot be resolved without more extensive decomposition and consideration of organizational consequences and impact.

A yes answer means that vulnerabilities are categorized and prioritized.

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

The mere identification of vulnerability is not sufficient for determining whether the organization should act to counter it. With the number of vulnerabilities growing exponentially (particularly for technology assets), no organization can (or would want to) address all of them. The organization must analyze vulnerabilities to determine which ones require additional attention.

Through vulnerability analysis, the organization seeks to understand the potential threat that the vulnerability represents. The structure of the vulnerability—what it can do, how it is exploited, the potential resulting effects—must be carefully considered in the context of the potentially affected assets and services. Vulnerability analysis includes activities to

- Understand the threat and exposure
- Review trend information to determine whether the vulnerability has existed before and what actions were taken to reduce or eliminate it
- Identify and understand underlying causes for exposure to the vulnerability
- Prioritize and categorize vulnerabilities for appropriate action to reduce or eliminate them
- Refer vulnerabilities to the organization's risk management process when more extensive consideration of the impact of the potential threat must be performed to determine an appropriate mitigation strategy

As a result of analysis, some vulnerabilities will be determined to be of no relevance to the organization (i.e., the organization is not exposed to them or the exposure is negligible). Other vulnerabilities will need to be addressed through a simple fix (such as a software patch or by turning off unnecessary services), while some will need to have a formal strategy developed. The organization should assign a course of action to each vulnerability.

A yes answer means that vulnerabilities are being analyzed to determine their importance and priority to the organization.

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

The organization establishes a vulnerability repository as the central source of vulnerability life-cycle information. As vulnerabilities are discovered, they are submitted to the organization's vulnerability repository by capturing the information in a format that is usable in the organization's vulnerability identification and analysis process. The repository is an essential construct that is vital to the efficiency and effectiveness of other operational resilience management processes. For example, accurate, complete, and timely information about vulnerabilities can assist in the examination of incidents and events, provide threat information to the risk management process for the identification of risks, and form the basis for root-cause analysis and trending for overall improvement of the operational resilience management process.

Basic information that should be collected about vulnerabilities include

- A unique organizational identifier for internal reference
- Description of the vulnerability
- Date entered to the repository
- References to the source of the vulnerability
- The importance of the vulnerability to the organization (critical, moderate, etc.)
- Individuals or teams assigned to analyze and remediate the vulnerability
- A log of remediation actions taken to reduce or eliminate the vulnerability

The vulnerability repository is a source of risk to the organization if accessed by unauthorized individuals. The organization should apply access controls to the vulnerability repository to permit only authorized individuals to view, modify, or delete information.

A yes answer means that a vulnerabilities repository is established and is kept current.

Goal 3 – Exposure to identified vulnerabilities is managed.

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

The organization must develop and implement an appropriate resolution strategy for vulnerabilities to which the organization has determined that exposure must be reduced or eliminated. This strategy can 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 (by eliminating the threat, the threat actor, and/or the motive)

Managing exposure to vulnerabilities will likely require a consideration of these actions and the ways that they can be realized through the development and implementation of appropriate strategies. Strategies may span a wide range of activities, including

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

The organization must also consider the need to integrate managing exposure to vulnerabilities with other related organizational processes such as change management, configuration management, product acquisition, and monitoring.

Strategies for managing exposure may also require a consideration of the impact of the action against the continuing operations of the organization. For example, to reduce exposure to a vulnerability, the organization may be required to turn off or eliminate certain operating system services that staff members may need to perform their job functions. The organization must either determine a workaround to the loss of this service or allow the service to continue operating with the implementation of detective controls (such as audit logging

and tracking) to ensure that it is not (or has not been) exploited by threat actors. Thus the organization's strategy may include the development and documentation of the workaround or the types and extent of detective controls that will be implemented.

A yes answer means that the organization has developed and implemented a resolution strategy for vulnerabilities to which the organization has determined that exposure must be reduced or eliminated.

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

Once the organization has developed a vulnerability management strategy, it must be monitored to ensure effective implementation and the achievement of results as documented in the strategy.

A yes answer means that the effectiveness of vulnerability mitigation is reviewed, and that review has been documented.

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

Unresolved vulnerabilities are regularly monitored and reported.

A yes answer means that unresolved vulnerabilities are documented and monitored.

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]

Root-cause analysis is a general approach for determining the underlying causes of events or problems as a means for addressing the symptoms of such events or problems as they manifest in organizational disruptions. Few vulnerabilities have organic causes (i.e., emerge on their own); instead, they are typically created by other actions or inactions such as poor software design, failure of organizational policies and processes, improper training, or operational complexity. Performing root-cause analysis allows the organization to look further into the reasons why exposures are occurring and to determine how to address these issues before they result in vulnerabilities that have to be analyzed and resolved.

A primary activity in root-cause analysis is to determine how to eliminate or reduce the underlying cause of exposures. Root-cause analysis may result in the development of strategies to address the root causes that are identified. As with developing strategies for managing vulnerabilities, this may include developing or improving controls as well as strategies for sustaining assets and services. It may also result in updating resilience training and awareness activities to ensure understanding of root causes and elimination of practices and processes that result in exposures. Overall, the identification and resolution of root causes can be used to improve the organization's operational resilience by ensuring that lessons learned are translated to knowledge.

Many tools and techniques for root-cause analysis exist. The organization must familiarize itself with these tools and techniques, select those that are most appropriate for use, and provide training to relevant staff in their use.

A yes answer means that underlying causes for vulnerabilities are identified (through root-cause analysis or other means), documented, and addressed.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing vulnerability management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for vulnerability management?

A policy is a written communication from the organization's senior management to employees.

The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for vulnerability management activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities.

Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have vulnerability management standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the vulnerability management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform vulnerability management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform vulnerability management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process.

Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned vulnerability management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan?

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

For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of vulnerability management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

MIL5-Defined

1. Has the organization adopted a standard definition of vulnerability management activities from which operating units can derive practices that fit their unique operating circumstances?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to vulnerability management activities documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

The incident management plan should address at a minimum:

- The organization's philosophy for incident management
- The structure of the incident management process
- The requirements and objectives of the incident management process relative to managing operational resilience
- A description of how the organization will identify incidents, analyze them, and respond to them
- The roles and responsibilities necessary to carry out the plan
- Applicable training needs and requirements
- Resources that will be required to meet the objectives of the plan
- Relevant costs and budgets associated with incident management activities

The organization should develop and document its plan for incident management and outline the specific objectives of the plan. The objectives of the plan should be translated into specific actions and assigned to individuals or groups to be performed when necessary.

A yes answer means that the organization has documented a plan of action that describes how it will respond to cyber security incidents that involve the critical service.

2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1]

The incident management process is also a source of knowledge that can be used by the organization to continually improve continuity plans and practices and strategies for protecting and sustaining services and assets.

A yes answer means that the plan is reviewed on a periodic basis.

3. Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]

The organization must identify the staff necessary to achieve the plan's objectives and ensure that staff are assigned and aware of their roles and responsibilities with respect to satisfying these objectives.

A yes answer means that staff are assigned to all roles and responsibilities defined in the incident management plan. An incomplete answer may be if staff are assigned even if there is no incident management plan.

4. Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]

Job descriptions (may also be called position descriptions) are a means to ensure that those who accept incident management roles and responsibilities are aware of their requirements.

A yes answer means that a detailed job description exists for each role and responsibility defined in the incident management plan. An incomplete answer may be if job descriptions include roles and responsibilities even if there is no incident management plan.

Goal 2 – A process for detecting, reporting, triaging, and analyzing events is established.

1. Are events detected and reported? [IMC:SG2.SP1]

Events must be captured and analyzed so that the organization can determine if the event will become (or has become) an incident that requires organizational action. The extent to which an organization can identify events improves its ability to manage and control incidents and their potential effects.

These are examples of methods of event detection:

- Monitoring of technical infrastructure, including network architecture and network traffic
- Reporting of problems or issues to the organization's service desk
- Observation of organizational managers and users of IT services
- Environmental and geographical events reported through media such as television, radio, and the internet
- Reporting from legal or law enforcement staff
- Observation of breakdown in processes or productivity of assets
- External notification from other entities such as CERT
- Results of audits or assessments

A yes answer means that an event report procedure exists to detect events and provide event reports to incident management staff and stakeholders.

2. Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]

Basic event (and incident) information should include:

- A unique identifier
- A brief description of the event
- An event category (denial of service, virus intrusion, physical access violation", etc.)
- The organizational 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 (application system, network segment, operating system, etc.)
- The individuals or teams to whom the event (or incident) was assigned
- Relevant dates
- The actions taken

Logging and tracking facilitates event triage and analysis activities, provides the ability to quickly obtain a status on the event and the organization's disposition, provides the basis for conversion from event to incident declaration, and may be useful in post-incident review processes when trending and root cause analysis is performed.

A yes answer means that the organization logs event data within a common repository, such as an incident database.

3. Are events categorized? [IMC:SG2.SP4]

Events may be categorized by type (e.g. security, safety, unauthorized access, user issue, denial of service, virus intrusion, physical access violation) and or by severity (e.g. critical, high, medium, low) or other categorization labels.

A yes answer means that events are consistently categorized according to a procedure and based on categories predefined by the organization.

4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]

Through triage, the organization determines the type and extent of an event (e.g., physical versus technical), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response.

A yes answer means that all cyber security events are analyzed in order to determine whether an event is related to other events which may indicate they are symptomatic of a larger issue, problem, or incident.

5. Are events prioritized? [IMC:SG2.SP4]

Events may be prioritized based on event knowledge, the results of categorization and correlation analysis, incident declaration criteria, and experience with past declared incidents.

A yes answer means that all events are prioritized based on established and available criteria.

6. Is the status of events tracked? [IMC:SG2.SP4]

Possible status types for event reports include:

- Closed
- Referred for further analysis
- Referred to organizational unit or line of business for disposition
- Declared as incident and referred to incident handling and response process

The status of events should be checked regularly to ensure that they are moving through the organization's established incident management process and are not stalled or awaiting activity. Events that need additional attention should be identified and resolved.

A yes answer means that the status of events is documented and is regularly reviewed.

7. Are events managed to resolution? [IMC:SG2.SP4]

Periodically review the incident knowledge base 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.

A yes answer means that there is a procedure to manage all events to closure.

8. Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]

An event may become an organizational incident that has the potential to be a violation of local, state, or federal rules, laws, and regulations. This is often not known early in the investigation of an event, so the organization must be vigilant in ensuring that all event and incident evidence is handled properly in case an eventual legal issue is raised.

A yes answer means that the organization has identified and documented rules, laws, regulations, and policies that govern evidence identification.

9. Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]

Rules, laws, regulations, and policies may require specific documentation for forensic purposes. Staff must be trained in proper identification and handling of evidence, ensuring that the integrity of the evidence is not altered.

A yes answer means that the organization has established event evidence handling procedures that align with its obligations, such as laws.

Goal 3 – Incidents are declared and analyzed.

1. Are incidents declared? [IMC:SG3.SP1]

Incident declaration defines the point at which the organization has established that an incident has occurred, is occurring, or is imminent, and will need to be handled and responded to.

Each organization has many unique factors that must be considered in determining when to declare an incident. Through experience, an organization may have a baseline set of events that define standard incidents, such as a virus outbreak, unauthorized access to a user account, or a denial-of-service attack. However, in reality, incident declaration may occur on an event-by-event basis.

A yes answer means that incidents are consistently declared according to an established procedure.

2. Have criteria for the declaration of an incident been established? [IMC.SG3.SP1]

To guide the organization in determining when to declare an incident (particularly if incident declaration is not immediately apparent), the organization must define incident declaration criteria.

Example criteria:

- 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 employees or external entities 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?
- Is the event common to the organization?
- Is the event isolated?
- Does the event constitute fraud or theft?
- Are there impacts such as damage to the organization's reputation?
- Is there a potential legal infraction?

A yes answer means that there is documented incident declaration criteria that is readily available to all staff who may need to declare an incident and that the criteria is developed as part of a standard procedure.

3. Are incidents analyzed to determine a response? [IMC:SG3.SP2]

Incident analysis should be focused on properly defining the underlying problem, condition, or issue and in helping the organization to prepare the most appropriate and timely response to the incident. It should also help the organization to determine whether the incident has legal ramifications.

Example incident analysis activities:

- Interviews with those who reported the underlying event(s)
- Interviews of specific knowledge experts

- Interviews of asset owners for assets affected by the incident
- 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 staff
- Consultation with legal and audit staff
- Consultation with product vendors and software/hardware suppliers
- Consultation with emergency management

A yes answer means that there is a standardized incident analysis procedure to formulate 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]

Incidents that the organization has declared and which require an organizational response must be escalated to those stakeholders who can implement, manage, and bring to closure an appropriate and timely solution. These stakeholders are typically internal to the organization (such as a standing incident response team or an incident-specific team) but could be external in the form of contractors or other suppliers. The organization must establish processes to ensure that incidents are referred to the appropriate stakeholders because failure to do so will impede the organization's response and may increase the level to which the organization is impacted.

A yes answer means that incidents are consistently escalated to appropriate stakeholders.

2. Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]

The organization's response to an incident must be founded on a well-structured incident response capability and plan. The actions related to incident response can include:

- Containing damage (i.e., by taking hardware or systems offline or by locking-down a facility)
- Collecting evidence (including logs and audit trails)
- Interviewing relevant staff (those involved in reporting or analyzing the incident and those affected by it)
- Communicating to stakeholders, including asset owners and incident owners
- Developing and implementing corrective actions and controls
- Implementing continuity and restoration plans or other emergency actions

Responding to incidents describes the actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. The range, scope, and breadth of the organizational response will vary widely depending on the nature of the incident. Incident response may be as simple as notifying users to avoid opening a specific type of e-mail message or as complicated as having to implement service continuity plans that require relocation of services and operations to an off-site provider.

A yes answer means that there are pre-planned actions such as invoking a service continuity plan, disaster recovery plan, or implementing other corrective actions that the organization takes to prevent or limit damage from an incident.

3. Are incident status and response communicated to affected parties? [IMC:SG4.SP3]

Miscommunications or inaccurate information about organizational incidents can have dire effects that far exceed the potential damage caused by an incident itself. As a result, the organization must proactively manage communications when incidents are detected and throughout their life cycle. This requires the

organization to develop and implement a communications plan that can be readily implemented to manage communications to internal and external stakeholders on a regular basis and as needed.

The incident communications plan should address at a minimum:

- The stakeholders with whom communications about incidents are required
- The types of media by which communications will be handled
- The various message types and level of communications appropriate to various stakeholders
- Special controls over communications (i.e., encryption or secured communications) that are appropriate for some stakeholders
- The roles and responsibilities necessary to carry out the plan
- The frequency and timing of communications
- Internal and external resources that are involved in supporting the communications process

These are examples of stakeholders that may need to be included in an incident communication plan:

- Members of the incident handling and management team or internal staff who have incident handling and management responsibilities
- Asset owners and service owners
- Information technology staff
- Middle and higher level managers
- Business continuity staff
- Affected customers or upstream suppliers
- Local, state, and federal emergency management staff
- Human resources departments, particularly if safety is an issue
- Communications and public relations 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, including newspaper, television, radio, and internet
- Regulatory and governing agencies
- Local utilities (power, gas, telecommunications, water, etc.), if affected.

A yes answer means that incident status and response is communicated to affected parties.

4. Are incidents tracked to resolution? [IMC:SG4.SP4]

Incidents that appear to be open for an extended period of time may not have followed the organization's incident management process or may not have been formally closed. The status of incidents in the incident database should be reviewed regularly to determine if open incidents should be closed or need additional action.

A yes answer means that there is a procedure to manage all 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]

Post-incident review should include a significant root-cause analysis process. The organization should employ commonly available techniques to perform root-cause analysis as a means of potentially preventing future incidents of similar type and impact.

A yes answer means that all incidents are analyzed after resolution to understand what caused them.

2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]

Considerations of other processes that may have caused or aided the incident should be given, particularly as they may exist in processes such as change management and configuration management.

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 between problem management and incident management strengthen the organization's overall ability to prevent incidents and minimize costly and reactive response activities.

From a risk management standpoint, using incident lessons learned to improve controls and protection strategies and optimize these strategies with continuity planning and response effectively shifts the organization's attention from a response mode to a preventive mode.

A yes answer means that incident information is used throughout other organizational processes, such as controls management or change management.

3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]

Lessons learned in incident management should serve as a benchmark for determining the validity and effectiveness of the organization's current strategies for protecting and sustaining assets. In addition, lessons learned should provide valuable information for continuous improvement of the incident management process.

These are examples of areas that need to be addressed after an incident:

- Update protection strategies and controls to protect assets and services from future incidents of similar type and nature.
- Update policies to reflect lessons learned.
- Update training for employees regarding the incident.
- Revise continuity plans and strategies to protect and sustain services and assets.
- Review and revise asset-level protection and sustainment requirements, if necessary.
- Revise incident criteria.
- Develop standardized responses to common incidents.
- Improve incident management processes

A yes answer means that actions are taken based on what is learned from incidents. This action may involve updating or implementing controls, revising policies, providing training, updating existing or developing new disaster recovery plans, etc.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing incident management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes:

- The process description
- Standards and requirements for the work products of the process

- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for incident management?

A policy is a written communication from the organization's senior management to employees.

The policy should address:
- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for incident management activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities. Examples of stakeholders include:
- Critical service owners
- Owners and custodians of assets
- 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

4. Have incident management standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the incident management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform incident management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:
- knowledge of tools techniques, and methods used to perform the process
- knowledge necessary to work effectively with asset owners and custodians
- knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform incident management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process.

Funding the process can include:
- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned incident management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:
- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:
- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are incident management activities periodically reviewed to ensure they are adhering to the plan?

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

For example, the review can include:
- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of incident management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers. Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process. Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

MIL5-Defined

1. Has the organization adopted a standard definition of incident management activities from which operating units can derive practices that fit their unique operating circumstances?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to incident management activities documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services)enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

The development of service continuity plans occurs as both a foundational and ongoing activity. Plans are developed at the time of service development and implementation but also on an ongoing basis as new risks are encountered and the operational environment changes. Typical work products include:

- Service continuity plan templates
- Service continuity plans (including relevant stakeholders)

A yes answer means that the organization has developed continuity plans for the critical service, and those plans include high-value assets (minimally people, information, technology, and facilities).

2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]

The organization should develop continuity plan templates that establish a standard for organizational planning. Such templates might include information about:

- Alternative activities that would have to be performed (technical or manual)
- Alternative resources and locations that would support the organization's high-value services
- Identification of vital staff roles and responsibilities
- High-value technology assets necessary to support the plan
- High-value information assets and vital records necessary to support the plan
- High-value facilities assets necessary to support the plan
- Relevant stakeholders of the plan and method of communicating with them
- Documentation of the recovery sequence for the service
- The restoration sequence for the service
- Security and access-related issues that are required to execute the plan
- Any special handling of information or technology that is required
- The test plan for the service continuity plan
- The service continuity training plan
- Coordination activities with other internal staff and external entities that must be performed to implement the strategy
- The levels of authority and access needed by responders to carry out the strategy and plan
- The cost of the plan and the activities necessary to carry out the plan
- The logistics of the plan

A yes answer means that the organization has developed standards for continuity plans, and the current plan for the critical service is derived from the standard.

3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]

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 to the organization or external (through outsourcing arrangements and service contracts). The organization must define the staff requirements that are required to meet the objectives of the plan, identify potential internal and external staff that will be needed to meet these requirements, and assign staff to activities in the plan. Where staff members do not have the necessary skill sets to meet the basic, minimum requirements of the plan, the organization must provide training and ascertain that the staff members are able to perform to the objectives stated in the plan as a result of this training

A yes answer means that the organization has assigned staff roles and responsibilities within continuity plans for the critical service.

4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]

Services depend on organizational assets, both internal and external, to ensure continuity of operations. They also rely on external partnerships such as public agencies and infrastructure such as public utilities and telecommunications. These dependencies and interdependencies must be identified in order to ensure a robust consideration of the range of planning that must be incorporated into the service continuity plans. Typical work products include:

- List of public service providers on which services depend (refer also to EC:SG4.SP3 and SP4)
- List of external entities, including business partners and vendors that facilitate service delivery
- Key contact list

A yes answer means that the organization has documented a list of key contacts within the continuity plans for the critical service, and that list is current.

5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]

The ability to execute service continuity plans during a disruption is related to their accessibility and viability. When service continuity plans that are developed but misplaced or are allowed to be changed at will, they are not usable by those who are responsible for executing them. Given that many service continuity plans are executed under emergency or crisis circumstances, the ability to know where the current version of the plans are stored is invaluable. To achieve this, the organization must take steps to ensure that the plans are archived, that the most current versions of the plans are available, that the plans are secured and free from intentional or unintentional modification, and that those who need to access the plans can readily retrieve them when necessary.

A yes answer means that the organization has collected continuity plans for the critical service and those plans are available to those who need to know.

6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]

The availability of a technology asset is paramount to supporting organizational services. Information that is stored, transported, or processed by technology assets may be accurate and complete, but if it is not available on demand or in a timely matter, the service may not be able to meet its mission.

There is a distinction between planned downtime and unplanned downtime. Planned downtime is usually the result of a user- or management-initiated event that has been subject to the change management process. Unplanned downtime typically arises from events or incidents outside the control of the organization such as

power outages, security breaches, and disasters like flooding or hurricanes. Unplanned downtime is the effect of diminished operational resilience.

A yes answer means that the organization has documented recovery time objectives for the high-value technology assets that support the critical service, and those are current.

Goal 2 – Service continuity plans are reviewed to resolve conflicts between plans.

1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]

Because of the sheer volume of service continuity plans and the operational interconnection of many services and assets, service continuity plans often overlap or place reliance on the same set of organizational resources. For example, an organization may have an offsite facility that is named in more than one plan as a backup site, but if more than one plan is executed simultaneously, the facility may not be able to satisfy requirements as prescribed in any single plan. More commonly, many people are often named in more than one service continuity plan that may need to be executed simultaneously. These types of conflicts must be identified and resolved. Typical work products include:

- Plan conflicts
- Plan updates and remediation actions

A yes answer means that the organization periodically reviews their collection of service continuity plans to ensure that they are actionable and do not conflict with each other.

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]

Having a test program and standards helps ensure regular and consistent testing of service continuity plans to ensure their viability during an event or emergency. Testing is conducted in a controlled and measured environment and is the only opportunity for the organization to know whether the plans it has developed will achieve the stated objectives and satisfy requirements.

The organization establishes the plan testing standards, structure, and reporting requirements. The testing program and standards are enforced for all plan owners and developers to ensure consistency, comparability, and ability to interpret results at the organizational level. In addition, a consistent schedule of plan testing is established based on factors such as risk, potential consequences to the organization, and other organizationally derived factors. A quality review capability is established to review the results of plan tests and to look for trends and other information that could be used in improving the general state of service continuity plans and the testing of plans. Typical work products include:

- Plan test program
- Plan test standards
- Plan test schedule

A yes answer means that the organization has developed standards for testing continuity plans, and ensures that tests adhere to those standards.

2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]

The test program and test standards should address the following, at a minimum:

- The organization's strategy for conducting service continuity plan tests
- The establishment of high-quality test objectives
- The level of involvement and commitment of plan stakeholders in the testing of the plan
- Reporting of test results

- Quality assurance review of test results
- Guidelines for addressing testing issues and concerns
- Guidelines on frequency of testing

A yes answer means that the organization has developed a schedule for testing continuity plans, and that schedule is used to test plans.

3. Are service continuity plans tested? [SC:SG5.SP3]

On a regular basis, service continuity plans are exercised (tested) according to their test plan. The test should establish the viability, accuracy, and completeness of the plan. It should also provide information about the organization's level of preparedness to address the specific area(s) included in the plan. The tests are performed under conditions established by the organization and the results of the test are recorded and documented.

A yes answer means that the organization tests continuity plans for the critical service.

4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]

The duplication and retention of information assets is a primary control for ensuring information asset availability. These controls not only must be applied to information assets that are critical to supporting high-value services, but also in the restoration of these services when disrupted.

In addition to performing backup and retention on information assets that support services, the organization also needs to address the retention and protection of its vital records—charters, articles of incorporation, customer contracts, employee records, etc. These information assets may not directly support a particular service, but they are critical to the overall continued viability of the organization and must be accessible particularly during disruptive events.

A yes answer means that the organization regularly tests information recovery strategies to ensure the availability of high value information assets that support the critical service.

5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]

The objective for developing and executing service continuity plan tests is to ensure that the plans work as intended, but also to identify required improvements to the plans and the 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 are also identified, documented, and incorporated into future tests.

A yes answer means that the organization evaluates results of critical service continuity plan tests against pre-determined objectives, and identifies improvements for the plan.

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]

The service continuity plans are executed, as organizational conditions require. Typical work products include:

- Organizational conditions for executing service continuity plans
- Documented results of executed service continuity plans

A yes answer means that the organization documents conditions that trigger execution of the continuity plans for the critical service.

2. Is execution of service continuity plans reviewed? [SC:SG6.SP2]

The debriefing of the execution of service continuity plans is an invaluable means for identifying plan shortcomings and for improving the plan. Plan improvements are documented through this process and incorporated into future plan versions. In some cases, new plans are developed in addition to or as replacements for existing plans. Logistical considerations of the plan are reviewed and analyzed, and changes are recommended. Unforeseen circumstances that arise during the execution of the plan—either due to the incident or the execution of the plan activities—are documented and addressed.

Typical work products:

- List of improvements to service continuity plans
- List of improvements to service continuity test plans

A yes answer means that the organization reviews the performance of continuity plans following execution.

3. Are improvements identified as result of executing service continuity plans? (SC:SG7.SP2)

Changes to service continuity plans are made as conditions dictate based on the change criteria established by the organization. The changes are made to existing service continuity plans (although new plans may result), and versions of existing plans are incremental according to the organization's versioning protocol and standards. Typical work products include:

- Baseline service continuity plans (established upon initial plan development)
- Updated service continuity plans (incremental version)
- Updated service continuity plan inventory/database

A yes answer means that the organization identifies improvements to the continuity plans for the critical service following reviews of performance.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing service continuity activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description. The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for service continuity?

A policy is a written communication from the organization's senior management to employees.

The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for service continuity activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities. Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have service continuity standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards).

Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the service continuity activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform service continuity activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities.

Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform service continuity activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process.

Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps

- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are service continuity activities periodically reviewed to ensure they are adhering to the plan?

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

For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of service continuity?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers. Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?**

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. **Are improvements to service continuity documented and shared across the organization?**

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

Operational risk is defined as the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

Risk sources are the fundamental areas of risk that can affect organizational services and associated assets while they are in operation to meet the organization's mission.

Identifying risk sources or areas of risk helps the organization to determine and categorize the types of operational risk that are most likely to affect day-to-day operations. The sources or areas of risk can be both internal and external to the organization.

Risk sources identify common areas where risks may originate. Typical internal and external sources 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, or risks posed by the complexity and unpredictability of interconnected systems
- Failures of technology, such as the unanticipated results of the execution of software and the failure of hardware components such as servers and telecommunications
- External events and forces, such as natural disasters, failures of public infrastructure, and failures in the organization's supply chain

A yes answer means that there is a documented list of operational risk areas.

2. Have categories been established for risks? [RISK: SG1.SP1]

Risk categories provide a means for collecting and organizing risk for ease of analysis and mitigation. Typical operational risk categories align with the various sources of operational risk such as failed processes, actions of people, systems and technology, and external events, but can be as granular as necessary for the organization to effectively manage risk. Operational risks may also align with the types of assets they are most likely to affect—risks to the availability of people, the confidentiality, integrity, and availability of information, etc.

A yes answer means that there is a documented list of risk categories.

3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]

The plan provides a common foundation for the performance of operational risk management activities (which are typically dispersed throughout the organization) and for the collection, coordination, and elevation of operational risk to the organization's enterprise risk management process.

Operational risk is defined as the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

Typical items addressed in an operational risk management strategy or plan include:

- The scope of operational risk management activities
- The methods to be used for operational risk identification, analysis,
- mitigation, monitoring, and communication
- The sources of operational risk
- How the sources of operational risk should be organized, categorized,
- compared, and consolidated
- Parameters for measuring and taking action on operational risks
- Risk mitigation techniques to be used, such as the development of
- layered administrative, technical, and physical controls and the
- development of service continuity plans
- Definition of risk measures to monitor the status of the operational risks
- Time intervals for risk monitoring and reassessment
- Staff involved in operational risk management and the extent of their
- involvement in the activities noted above

A yes answer means that there is a documented strategy or plan for managing operational risks and this strategy document is being used to guide the risk management effort.

4. Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]

The strategy should be documented and communicated to all relevant stakeholders, internal and external, who are responsible for any operational risk management activity.

Operational risk is defined as the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events.

A yes answer means that all of the relevant stakeholders have been determined and the plan for managing operational risk has been communicated to them.

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]

Organizational impact areas identify the risk categories where realized risk may have meaningful and disruptive consequences. These areas typify what is important to the organization and to the accomplishment of its mission.

Examples of organizational impact areas:

- Reputation and customer confidence
- Financial health and stability
- Staff productivity

- Safety and health of staff and customers
- Fines and legal penalties
- Compliance with regulations

A yes answer means that there is a documented list of impact areas.

2. Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]

The prioritization of impact areas allows the organization to determine the relative importance of these areas to allow them to be used for risk prioritization and mitigation.

A yes answer means that the impact areas are prioritized.

3. Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]

The range of risk measurement criteria (tolerance parameters) can be either qualitative (high, medium, low) or quantitative (based on levels of loss, fines, number of customers lost, etc.).

Additional Information:

Risk measurement and evaluation criteria provide the bounds on the severity of consequences to the organization across the organizationally defined areas of impact. The consistent application of these criteria across all operational risks ensures that risks are prioritized according to organizational importance (even if they are specific to an organizational unit or line of business) and are mitigated accordingly.

A yes answer means that the operational risk tolerance parameters are defined and documented for each area of impact. If operational risk tolerance parameters are not defined for all areas of impact then an incomplete score would be appropriate.

4. Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]

Risk parameters provide the organization a means for consistent measurement of operational risk across the organization.

Risk thresholds are a management tool to determine when risk is in control or has exceeded acceptable organizational limits. They must be set for each category of operational risk that the organization establishes as a means for measuring and managing risk. For example, a risk threshold for virus intrusions may be whenever more than 200 users are affected; this would indicate that management needs to act to prevent operational disruption.

A yes answer means that the operational risk thresholds are defined and documented for each category of risk.

Goal 3 – Risks are identified.

1. Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]

Operational risks that can affect assets such as people, information, technology, and facilities must be identified and mitigated in order to actively manage the operational resilience of these assets and, more importantly, the services to which these assets are connected.

The disruption of asset productivity due to operational risk affects the ability of associated services in meeting their mission. Thus, risks associated with organizational assets must be examined in the context of these services to determine if there is a potential impact on mission assurance, which in turn could affect the organization's ability to meet its mission. Examining risk in the context of services provides the organization additional information that must be considered when prioritizing risks for disposition and mitigation.

A yes answer means that there is a documented and complete list of operational risks by service that is defined.

Goal 4 – Risks are analyzed and assigned a disposition.

1. Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]

Each risk is evaluated and assigned values in accordance with the defined risk parameters and risk measurement criteria. (These include likelihood, consequence, consequence severity, and thresholds.) The organization may weight the valuation of the risks by adjusting for the priority of impact areas (reputation, finance, etc.) that they established as part of the risk measurement criteria. This will ensure that impact areas of most importance to the organization will influence more strongly which risks are prioritized higher for mitigation. The organization can further influence the prioritization by applying a probability factor, if known.

The valuation can be qualitative (high, medium, or low) or can be a quantitative relative risk score that combines likelihood, impact area weighting, and consequence value. The valuation assigned to the risk statement will be used as a factor in deciding what to do with the risk.

A yes answer means that there is a documented value of impact assigned for all identified risks associated with the critical service.

2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]

An important part of risk management is to determine a strategy for each identified risk and to implement actions to carry out the strategy. Strategy development begins with assigning a risk disposition to each risk, that is, a statement of the organization's intention for addressing the risk.

Assign a risk disposition to each risk statement based on risk valuation and prioritization. A risk disposition is assigned to each risk statement or group of statements. The organization must establish a range of acceptable and consistent risk dispositions and their definitions.

Possible risk dispositions include:

- Avoid
- Accept
- Monitor
- Research or defer
- Transfer
- Mitigate or control

A yes answer means that there is a documented disposition assigned for identified risks associated with 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]

Risk mitigation requires the organization to perform two distinct actions: (1) develop risk mitigation plans and (2) implement and monitor these plans for effectiveness.

Risk mitigation involves the development of strategies that seek to minimize the risk to an acceptable level. This includes 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

Developing risk mitigation plans is an extensive activity that will vary by organization. There are some common elements of risk mitigation plans that should be considered for all plans:

- How the threat or vulnerability will be reduced
- The actions that will prevent or limit an actor from exploiting a threat or vulnerability
- The controls that will need to be implemented or updated to reduce exposure, including an articulation of administrative, physical, and technical controls
- The service continuity plans that would be used to reduce the impact of consequences should risk be realized
- The staff who are responsible for implementing and monitoring the mitigation plan
- The cost of the plan, and a cost-benefit analysis that demonstrates the value of the plan commensurate with the value of the related assets and services or avoidance of consequences
- The implementation specifics of the plan (when, where, how)
- The residual risk that would not be addressed by the plan

A yes answer means that there is a documented mitigation plan for all identified risks that the organization decides to mitigate.

2. Are identified risks tracked to closure? [RISK: SG5.SP2]

Effective management and control of risk requires the organization to monitor risk and the status of risk strategies. Because the operational environment is constantly changing, risks identified and addressed may need to be revisited, and a new disposition and strategy may need to be developed. The risk management strategy defines the intervals at which the status of risk strategies must be revisited.

The implementation of risk strategies requires the monitoring of risks according to their disposition and the implementation and monitoring of risk mitigation plans.

The disposition for risks that are not being mitigated must be periodically assessed and revised as necessary. Some risks may, under future circumstances, require the development of a mitigation plan.

A yes answer means that there is an updated and complete list of risks, with current status and it is used to track risks to closure.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing risk management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description. The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for risk management?

A policy is a written communication from the organization's senior management to employees. The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines

- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for risk management activities have identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities. Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have risk management activities standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards). Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the risk management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform risk management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities. Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform risk management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process. Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are risk management activities periodically reviewed to ensure they are adhering to the plan?

This review is often done by an independent entity (either internal or external to the organization). For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of risk management?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers.

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process. Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to risk management documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

The purpose of the catalog of external dependencies is to support the identification and prioritization of external dependencies and the management of risks associated with selected dependencies.

The organization's external dependencies will change over time as a result of changes to relationships with essential suppliers and customers, changes in services, the life cycle of assets, and many other reasons. 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:

- List of external dependencies and entities
- Documented process for updating the list of external dependencies and entities

A yes answer means that the organization has documented external relationships that affect the critical service.

2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]

The data that is collected, stored, and routinely updated as part of defining an external dependency and its corresponding external entity is used to help prioritize the external dependency and identify risks associated with the external dependency. The data fields should therefore be set in consideration of the criteria, thresholds, and process for prioritizing external dependencies and in consideration of the risk identification process for external dependencies.

A yes answer means that the organization has established a process for identifying external dependencies, and that process is followed.

3. Are external dependencies prioritized? [EXD:SG1.SP2]

The prioritization of external dependencies must be performed to ensure that the organization properly directs its operational resilience resources to the external dependencies that most directly impact and contribute to services that support the organization's mission. These external dependencies require the organization's direct attention because their disruption has the potential to cause the most significant organizational consequences. External dependency prioritization is performed relative to the critical service—that is, external dependencies associated with critical services are those that must be given the highest priority for operational resilience activities.

However, the organization can use other criteria to establish high-priority external dependencies, such as:

- Actions of the external entity in the support, maintenance, or custodial care of high-value organizational assets
- The extent to which the organization would rely on the actions of the external entity during off-normal operations, crises, or other times of operational stress
- Actions of the external entity in supporting the organization's resilience process
- An external dependency resulting from external entity access to highly sensitive or classified information or to the organization's trade secrets or proprietary information such as intellectual property
- External dependencies that are of high value to more than one service
- Actions of the external entity in developing, providing, or commissioning new assets for the organization
- The organization's tolerance for "pain"—the degree to which it can suffer degraded performance of the external dependency and continue to meet its mission

Typical work products include:

- Criteria for prioritizing external dependencies
- Prioritized list of external dependencies
- Results of external dependency affinity analyses

A yes answer means that the organization has a prioritized list of external dependencies that affect the critical service, and that list is current.

Goal 2 – Risks due to external dependencies are identified and managed.

1. Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]

Risks due to external dependencies must be identified and assessed so that they can be effectively managed to maintain the resilience of the organization's high-value services.

The identification of risks due to external dependencies forms a baseline from which a continuous risk management process can be established and managed. Typical work products include:

- External dependency risk statements, with impact valuation
- List of external dependency risks, with categorization and prioritization

A yes answer means that the organization has identified risk associated with external dependencies, and that list has been prioritized and is current.

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]

For each external dependency, the organization should establish a detailed set of specifications that the external entity must meet in order to support and extend the resilience of the organization's operations. Related resilience requirements are reflected in the specifications. It is important that these specifications be thorough, detailed, definitive, adequate for use as criteria when selecting external entities, suitable as language in agreements with external entities, and appropriate for use as a basis for monitoring the performance of the external entity.

When developing specifications for external dependencies, the organization should:

- Consider the type of organizational assets or services impacted by the external dependency and their importance to the organization's mission and operations
- Understand the extent to which the external entity takes custodial control of the organization's assets,

and any resilience requirements of those assets that must be satisfied
- Consult internal and external stakeholders responsible for the associated assets and services
- Be aware of other assets or services that may rely upon the same external dependency and entity (as would be indicated by the affinity analysis in EXD:SG1.SP2)
- Review the resilience requirements established in the Resilience Requirements Development process area for the assets or services in question
- Review and select appropriate resilience guidelines established in the Resilient Technical Solution Engineering process area for the development of all software and system assets
- Include the enterprise-level specifications

The resilience specifications for an external dependency must clearly cover the resilience requirements of the assets or services that rely on the external entity. They should also include key features and capabilities of the external entity.

Typical work products include:
- Documented resilience specifications
- Service level agreements

A yes answer means that the organization communicates resilience requirements for assets (people, information, technology, facilities) that support the critical service within agreements with external parties.

2. Are these requirements reviewed and updated? [EXD:SG3.SP2]

Periodically review and update resilience requirements that relate to for external dependencies and entities as conditions warrant.

A yes answer means that the organization monitors the status of resilience obligations established in agreements with external parties to ensure that they are current.

3. Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]

External entities should be selected according to an organized and thorough process and according to explicit specifications and selection criteria. The selection process and criteria should be designed to ensure that the selected entity can fully meet the organization's specifications as established. Related resilience requirements are reflected in the specifications.

Typical work products include:
- Requests for proposals or other types of external entity solicitation documents that include specifications in cases in which proposals and bids are being sought by the organization
- External entity selection criteria
- Evaluation of each external entity proposal against the selection criteria
- Selection decision and supporting rationale

A yes answer means that the organization evaluates operating partners based upon their ability to meet the resilience requirements of assets that support the critical service.

4. Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]

Types of agreements may include contracts, memoranda of agreement, purchase orders, and licensing agreements. In some cases, agreements such as mutual-aid agreements may spell out what services a public authority provides for the organization during normal operations and during crises. In cases in which the external entity and the organization are part of the same legal entity or share a common parent legal entity, the organization or the parent entity may have special procedures for establishing and enforcing agreements.

Agreements are often composed from multiple sections or multiple documents, each of which describes some aspect of the arrangement and agreement. In all cases, the agreement, regardless of form, should:

- Be enforceable by the organization
- Include detailed and complete specifications that must be met by the external entity
- Include any required performance standards or work products from the organization
- Be changed to reflect changes in specifications over the life of the relationship

A yes answer means that the organization includes resilience requirements within agreements with external entities that support the critical service.

Goal 4 – Performance of external entities is managed.

1. Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]

The performance of external entities against the agreement terms and specifications—particularly those focused on the organization's assets and services resilience requirements—must be periodically monitored. This includes all external dependencies for which the entity is responsible. The organization uses the specifications and formal agreements as the basis and criteria for monitoring the external entity. Any deviations must be analyzed to understand the potential impact on the organization.

A yes answer means that the organization periodically monitors the performance of external entities that support the critical service against identified resilience requirements.

2. Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]

To ensure that performance monitoring is performed on a timely and consistent basis, the organization should establish procedures that determine the frequency, protocol, and responsibility for monitoring a particular external entity. (Responsibility is typically assigned to the organizational owner of the relationship.) These procedures should be consistent with the terms of the agreement with the external entity It may be appropriate to adjust the monitoring frequency in response to changes in the risk environment, changes to external dependencies, or changes in the external entity.

A yes answer means that the organization has assigned staff with the responsibility of monitoring external entities, and monitoring is currently being conducted as needed.

3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]

Implementing corrective actions is a necessary part of managing external entity performance. The objective of any corrective action is to minimize the disruption to the organization's operation or the risk of any such disruption based on external dependencies. The range of corrective actions should be established in the agreement with the external entity, and an evaluation of alternatives should be completed prior to implementing corrective actions.

In cases in which the external entity is developing or otherwise providing an asset or assets to the organization, the appropriate corrective action may be to reject the delivery of the assets.

Typical work products include:

- Corrective action reports or documentation

- Correspondence with an external entity documenting corrective actions

A yes answer means that the organization is prepared to take corrective actions based on identified issues related to the performance of external entities that support the critical service, or has taken corrective action in the past based on issues with meeting critical service resilience requirements.

4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]

Implementing corrective actions is a necessary part of managing external entity performance. The objective of any corrective action is to minimize the disruption to the organization's operation or the risk of any such disruption based on external dependencies. Corrective actions should be documented in accordance with specifications in the agreement and used to inform and improve ongoing monitoring of the external entity.

A yes answer means that the organization evaluates corrective actions enforced on external entities that support the critical service in order to ensure that issues related to meeting resilience requirements are remedied.

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]

Because they are geographically static, facilities rely on public services that are in operation in the immediate environment in which the facility exists. These public services may be vital to the facility's continued operation during a disruption and, by default, to the services that are performed in the facility. Thus, a thorough consideration of these services must be given for service continuity planning and incorporated into requisite service continuity plans. Public services generally include services that are specific to the geographical region of the facility and are financed by public funds. (In some cases, depending on the organization and its size, these services may have been privatized and therefore may be financed by and under the direct control of the organization.) Public services include:

- Fire response and rescue services
- Local and, in some cases, federal law enforcement (police, National Guard, FBI, etc.)
- Emergency management services, including paramedics and first responders
- Other services, such as animal 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

A yes answer means that the organization has identified and documented the public services on which the critical service depends, and the list is current.

2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]

Facility assets are a primary point where an organization intersects physically with its geographical environment. Facilities are vitally dependent on public infrastructure and services to operate and to remain viable. These services include telecommunications and telephone services, electricity, natural gas, and other energy sources, water and sewer services, trash collection and disposal, and other support services. These dependencies must be carefully evaluated for several reasons. First, the organization must be prepared to address the loss of these services, which can affect organizational services that are supported by a facility. Second, the organization may need to consider the resilience of public services when developing service

continuity plans for a facility—the inability to retain telecommunications, power, or water services may adversely affect the organization's ability to execute the facility's service continuity plan. Considerations of these public services may also cause the organization to make decisions about capital improvements (such as implementing backup power systems) that would be necessary to ensure a minimal level of operational resilience for the facility.

Typical work products include:

- Results of business impact analysis (documenting public infrastructure dependencies for facilities)
- List of public infrastructure providers on which facilities are dependent
- Key contact list
- Updated service continuity plans

A yes answer means that the organization has identified and documented infrastructure providers on which the critical service depends, and the list is current.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing external dependency management activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description. The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for external dependency management?

A policy is a written communication from the organization's senior management to employees. The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for external dependency management activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities. Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have external dependency management activities standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards). Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the external dependency management activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform external dependency management activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities. Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform external dependency management activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process. Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of external dependency management activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. **Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results?**

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. **Are external dependency management activities periodically reviewed to ensure they are adhering to the plan?**

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

For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. **Is higher-level management aware of issues related to external dependency management?**

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers. Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process. Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?**

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to external dependency management documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

9 Training and Awareness

The purpose of training and awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational sustainment and protection.

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]

To establish an effective awareness program, an organization must identify awareness needs and establish a plan and capability to meet those needs.

Awareness needs reflect the message that is to be communicated regarding resilience to all parties, internal and external, that have a vested interest in the resilience activities of the organization. Awareness needs are derived by determining the set of resilience topics, plans, issues, or policies of which various sets of the organization's population need to be kept aware.

Awareness sources include:

- Resilience requirements (protection and sustainment requirements for assets and services)
- Organizational policies
- Vulnerabilities
- 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 communications plans
- Event reporting procedures

A yes answer means that there is a documented list of awareness needs for staff connected to the critical service.

2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]

Baseline competencies may be as detailed as the organization needs to describe its required skill sets. This may involve many layers of information, including:

- Role (security administrator, network administrator, CIO, etc.)
- Position (CIO, senior security analyst, network engineer, 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)

In order to determine what skills the organization must possess to meet its cyber security needs, baseline competencies must be established relative to the resilience program and plan to ensure the entire range of necessary skills are identified.

The baseline competencies represent the staffing and skill set needs relative to carrying out the organization's resilience program and plan. The baseline competencies should be based on what the organization needs, not what it currently has in terms of staff and skills. By determining what the organization needs, the appropriate target for a sufficient level of staffing and skills is established.

A yes answer means that there is a documented list of skills (by role) necessary to meet the needs of the organization's critical service.

3. Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]

The organization must determine what skills it currently possesses in its pool of available human resources and identify skill gaps that can affect its ability to manage operational resilience.

Skill gaps and deficiencies expose the areas where the organization does not have the expertise, aptitude, skill, or experience to meet current needs. These gaps can result in risks to the organization in that significant resilience activities may not be performed appropriately or may not be performed at all.

A yes answer means that there is a documented list of skill gaps (by role) that must be addressed to meet the needs of the organization's critical service.

4. Have training needs been identified? [OTA:SG3.SP1]

Training needs are established by identifying people in the organization with resilience roles and responsibilities and analyzing gaps in their knowledge and skills that need to be addressed in order for them to succeed in their roles.

The training needs should focus not only on the skills and knowledge needed to perform particular roles in the supporting disciplines of security, business continuity, and IT operations and service delivery, but also on the convergence aspects of these disciplines toward operational resilience management.

These are examples of sources of resilience 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 human resource management process
- The process of service continuity
- The organization's compliance management process
- The organization's incident management process
- Training needs for external parties

A yes answer means that there is a documented list of training needs to address all of the skill gaps identified by the organization for the critical service.

Goal 2 – Awareness and training activities are conducted.

1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]

Awareness activities must meet the broad needs of staff members, and the logistics of performing these activities must be planned. The activities must be scheduled, advertised (if necessary), and resourced.

Typical work products include:

- Awareness activity materials
- Awareness activity schedules
- Awareness activity logistics
- List of staff responsible for each awareness activity

A yes answer means that cyber security awareness activities for the critical service are conducted to address all of the identified awareness needs.

2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]

Training should be planned and scheduled. Training is provided that has a direct bearing on the expectations of work performance. Therefore, optimal training occurs in a timely manner with regard to imminent job-performance expectations.

Typical work products include:
- Delivered training courses
- Training schedule

The organization must perform resilience training to ensure that staff is appropriately skilled in their roles to support the operational resilience management process. Training must be delivered according to the training plans developed and must address the vast range of needs represented in the operational resilience management process.

Training is tied to work responsibilities so that on-the-job activities or other outside experiences will reinforce the training within a reasonable time after the training.

A yes answer means that training activities for the critical service are conducted to address all of the identified training needs of staff associated with the critical infrastructure service.

3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]

A process should exist to determine the effectiveness of the training and awareness programs for meeting the training and awareness needs of staff involved in the operational resilience management process.

Examples of methods to evaluate the effectiveness:
- Testing
- Post-training surveys
- Questionnaires
- Focus groups
- Selective interviews
- Behavioral measures (password strength could be evaluated before and after a password-awareness activity.)
- Observations, evaluations, and benchmarking activities

A yes answer means that the effectiveness of the training and awareness programs for the critical service is evaluated for effectiveness.

4. Are awareness and training activities revised as needed? [OTA:SG1.SP3 and OTA:SG3.SP3]

Capabilities for implementing the training and awareness 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, and revising the awareness capability as needed.

Situations in which training and awareness materials may need to be revised:
- Training needs change (e.g. new technology is available)
- An evaluation of the training identifies the need for change
- Changes in existing awareness needs and requirements
- Emergence of new awareness needs and requirements
- Assessment of effectiveness of awareness presentations
- Training refresh

A yes answer means that all the security training and awareness activities are revised as needed and that updated training and awareness materials and work products are produced.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing training activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description. The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for training?

A policy is a written communication from the organization's senior management to employees. The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for training activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities. Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have training standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented. Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards). Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality. Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of the training activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process

performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform training activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities. Examples of knowledge and skills needed include:

Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform training activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process. Funding the process can include:
- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:
- Identifying asset-level and service-level risks
- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. Are training activities periodically reviewed and measured to ensure they are effective and producing intended results?

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:
- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. Are training activities periodically reviewed to ensure they are adhering to the plan?

This review is often done by an independent entity (either internal or external to the organization). For example, the review can include:
- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers

- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. Is higher-level management aware of issues related to the performance of training?

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers.

Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process.

Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

MIL5-Defined

1. Have the organization adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances?

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to training documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

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]

Monitoring is not simply a process of accumulating data; instead, it is a process of data collection and distribution with the purpose of providing timely, accurate, complete, and useful information about the current state of operational processes, any potential threats or vulnerabilities, and information about the effectiveness of the critical service's operational resilience management activities. In order to accomplish these tasks a person must be assigned responsibility for the monitoring program.

A yes answer means that responsibility has been assigned and documented, and is current.

2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]

Effective monitoring requires people, procedures, and technology that need to be deployed and managed to meet monitoring requirements and provide timely and accurate information to other operational resilience management procedures. This

requires the establishment of appropriate infrastructure to support the procedures, collection standards and procedures to ensure consistency and accuracy of information, the active collection of data, and the distribution of data to relevant stakeholders.

A yes answer means that procedures have been developed and implemented.

3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3]

The service's 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, the funding required for monitoring procedures, and any training or skills improvement activities that will be needed to meet requirements.

A yes answer means that resources have been assigned and trained to monitor threats to the critical infrastructure service.

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]

There are many types of stakeholders that require communications related to managing operational resilience. These stakeholders may be very diverse depending on the type of communications needs they

have, the frequency of the communications (whether discrete or continuous, circumstantial, or ongoing), and the level of communications necessary (notifications, press releases, crisis communications, etc.). Understanding the level and extent of stakeholders helps to effectively develop and satisfy communications requirements.

These are examples of internal stakeholders that may need to receive communications:

- Members of the incident handling and management team (if the organization has established such a team) or internal staff who have incident handling and management job responsibilities
- Shareholders
- Asset owners and service owners
- Information technology staff
- Middle and higher level managers
- Business continuity staff (if they will be required to enact continuity or restoration plans as a result of an incident)
- Human resources departments, particularly if safety is an issue
- Communications and public relations staff
- Staff involved in governance and oversight functions
- Support functions such as legal and audit

A yes answer means that internal stakeholders related to cyber security threat information 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]

These are examples of external stakeholders that may need to receive communications:

- Legal and law enforcement staff as required
- External media outlets, 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, if affected
- Regulatory and governing agencies

A yes answer means that external stakeholders related to cyber security threat information have been identified and documented.

Goal 3 – Threat information is communicated.

1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]

Threat information communications must be delivered on an as-needed basis, according to established requirements. Because threat information communications can be diverse, a broad array of procedures, practices, technology, and infrastructure to support those requirements may need to be developed and implemented. Various communications methods and channels (as appropriate to support requirements) should be considered and identified; and an infrastructure (physical and technical) to support those methods and channels be developed and implemented. Through these actions timely, relevant, consistent, high-quality, and purposeful communications can be delivered proactively or during an event, incident, or crisis.

A yes answer means that the organization ensures that threat information is effectively communicated to identified stakeholders.

2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]

Managing communications requires that a communications plan be established that addresses the unique and specific needs that arise from the procedures involved in managing operational resilience. The communications plan is carried out through a communications program that is staffed with resources that are properly trained and authorized to develop, implement, and manage communications processes and specifically meet the needs of resilience communications.

A yes answer means that resources have been assigned and have the associated authority and accountability for communicating cyber security threat information to stakeholders.

3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]

Regardless of the communications type, training (sometimes specialized) must be provided to staff that support and enable communications procedures. This may begin with a skills inventory and gap analysis so that effective training programs can be identified and used.

A yes answer means that resources have been trained in communicating cyber security threat information affecting the critical service.

Maturity Indicator Levels

MIL2-Planned

1. Is there a documented plan for performing situational awareness activities?

The plan for performing the process is created to ensure that the process is performed according to an established process description.

The plan typically includes:

- The process description
- Standards and requirements for the work products of the process
- Objectives for performing the process
- Dependencies among the activities
- As well as other components that would be in a project plan such as, resources, work products, assignments of responsibility, etc.

2. Is there a documented policy for situational awareness?

A policy is a written communication from the organization's senior management to employees. The policy should address:

- Responsibility, authority, and ownership for performing process activities
- Procedures, standards, and guidelines
- The development of criteria to provide guidance
- Methods for measuring adherence to policy, exceptions granted, and policy violations

3. Have stakeholders for situational awareness activities been identified and made aware of their roles?

Stakeholders need to be identified and understand their appropriate involvement. These stakeholders include those who are suppliers of inputs to the process, users of the outputs, and performers of process activities.

Examples of stakeholders include:

- Critical service owners
- Owners and custodians of assets
- 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

4. Have situational awareness standards and guidelines been identified and implemented?

Standards and guidelines, both industry and organizational, are identified and implemented.

Standards are formal requirements developed and used to prescribe consistent approaches (for example, ISC/IEC standards, IEEE standards and organizational standards). Guidelines may be issued by and used by an organization to make the actions of its employees more predictable, and presumably of higher quality.

Standards and guidelines are typically referenced in organizational policies.

MIL3-Managed

1. Is there management oversight of the performance of situational awareness activities?

Activities, status, and results of the performance of the process are reviewed with the immediate level of management responsible for the process. These reviews provide management visibility into the process performance based on day-to-day process activities. Corrective actions are taken when the actual results and performance deviate significantly from expected results and performance.

2. Have qualified staff been assigned to perform situational awareness activities as planned?

Responsibility and authority for performing specific tasks of the process are assigned. In addition, the criticality of the service requires that staff members assigned to the process have appropriate knowledge and skills to perform the process activities. Examples of knowledge and skills needed include:

- Knowledge of tools techniques, and methods used to perform the process
- Knowledge necessary to work effectively with asset owners and custodians
- Knowledge necessary to work effectively with stakeholders

3. Is there adequate funding to perform situational awareness activities as planned?

Consideration for funding the process should go beyond the initial establishment of the process to the maintenance of the process. Funding the process can include:

- Defining funding needs
- Establishing a budget
- Resolving funding gaps
- Funding the process activities
- Tracking and documenting costs

4. Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled?

Failed internal processes can impact operational resilience. Risks associated with internal processes need to be managed effectively through exercising a risk management process. This includes:

- Identifying asset-level and service-level risks

- Assigning categories (e.g., by asset type), priorities, and disposition
- Mitigation and control of risks

MIL4-Measured

1. **Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results?**

Activities that are a part of the defined process should be evaluated in order to ensure that they continue to achieve their objective(s). Examples of measures might include:

- The number of times an activity is performed
- The quality of a particular work product
- Schedule
- Budget

Problems in the process plan or in the execution of the process are identified.

2. **Are situational awareness activities periodically reviewed to ensure they are adhering to the plan?**

This review is often done by an independent entity (either internal or external to the organization). For example, the review can include:

- Assuring that the process has been followed
- Verification of process controls
- Process reports and reviews are used to inform decision makers
- Responsibility, accountability, and authority for process activities are assigned
- Non-compliance is addressed
- Needed process maintenance is identified when expected results or outputs are not met

3. **Is higher-level management aware of issues related to situational awareness?**

Higher-level managers belong to a level of management in the organization above the immediate level responsible for the process and can be senior managers. Different managers have different needs for information about the process. These reviews are typically briefings presented by those responsible for the process. Examples of presentation topics include:

- Schedule status for achieving significant milestones
- High impact risks associated with the process
- Process areas for improvement

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?**

The organization has a set of standard processes that are made available to organizational units. Organizational units can then select from these standard processes to establish their processes.

The difference between MIL5 and the lower MIL levels is that the standards, process descriptions, and procedures of the critical service are tailored from the organization's set of standard processes to suit the critical service and are more consistent across different organizational units (or services). This allows organization-wide process improvements and organization-wide learning from experiences.

2. Are improvements to situational awarene¥ss activities documented and shared across the organization?

Process related experiences, including information and artifacts derived from performing the process, are collected and stored in an organizational repository. Examples of process related experiences include work products, measures, and lessons learned. In addition, actively collecting improvements to process activities from organizational units (or services) enables the sharing of improvements across the organization and making improvements to the organization's set of standard processes which results in continuous process improvement.

Homeland Security